

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号  
特開2002-374261  
(P2002-374261A)

(43) 公開日 平成14年12月26日 (2002. 12. 26)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	ターマコード* (参考)
H 0 4 L 12/28	3 0 0	H 0 4 L 12/28	3 0 0 Z 5 K 0 3 3
G 0 6 F 1/00	3 7 0	G 0 6 F 1/00	3 7 0 E 5 K 0 6 7
H 0 4 Q 7/38		H 0 4 B 7/26	1 0 9 R

審査請求 未請求 請求項の数30 O L (全 28 頁)

(21) 出願番号 特願2001-183315(P2001-183315)

(22) 出願日 平成13年6月18日 (2001. 6. 18)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 松野 克巳

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 100082131

弁理士 稲本 義雄

Fターム(参考) 5K033 BA01 CC01 DA17

5K067 AA34 BB04 BB21 DD17 DD30

EE02 EE12 HH22

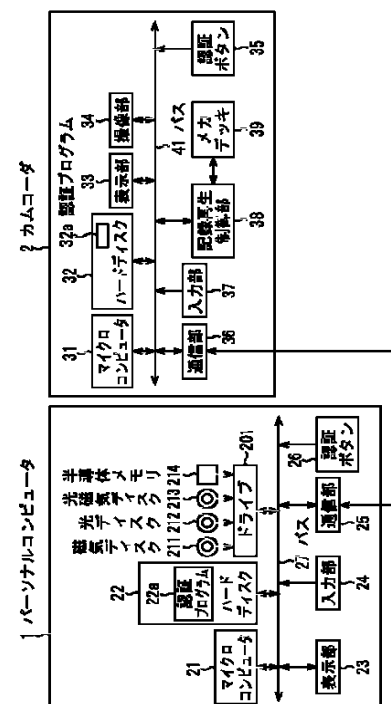
(54) 【発明の名称】 情報処理装置および方法、情報処理システム、記録媒体、並びにプログラム

(57) 【要約】

【課題】 ブルートゥースによる電子機器間の相互認証を容易に実現させる。

【解決手段】 ユーザは、パーソナルコンピュータ1とカムコーダ2の相互認証をさせるとき、双方の認証ボタン26、35を同時に押下する。その結果、パーソナルコンピュータ1の認証プログラム22aと、カムコーダ2の認証プログラム32aは、相互の認証ボタン26、35がオンにされた時刻とオフにされた時刻を検出し、相互にその時刻の情報を交換して、所定の時間差の範囲内で一致すると判定するとき、相互に認証処理がなされているものとみなし、認証を認める。

図4



【特許請求の範囲】

【請求項1】 ネットワークを介して他の情報処理装置と接続される情報処理装置において、

オンオフを入力する入力手段と、

前記入力手段によりオンが入力された第1のタイミングを計測する第1のタイ

ミング計測手段と、前記入力手段によりオフが入力された第2のタイミングを計測する第2のタイミング計測手段と、

前記第1のタイミング、および、前記第2のタイミングを前記ネットワークを介して他の情報処理装置に送信する送信手段とを備えることを特徴とする情報処理装置。

【請求項2】 前記ネットワークは、ブルートゥースにより構成されることを特徴とする請求項1に記載の情報処理装置。

【請求項3】 前記第1のタイミング計測手段、および、前記第2のタイミング計測手段は、いずれも複数回数のタイミングを計測することを特徴とする請求項1に記載の情報処理装置。

【請求項4】 ネットワークを介して他の情報処理装置と接続される情報処理装置の情報処理方法において、オンオフを入力する入力手段と、

前記入力ステップの処理でオンが入力された第1のタイミングを計測する第1のタイミング計測ステップと、

前記入力ステップの処理でオフが入力された第2のタイミングを計測する第2のタイミング計測ステップと、

前記第1のタイミング、および、前記第2のタイミングを前記ネットワークを介して他の情報処理装置に送信する送信ステップとを含むことを特徴とする情報処理方法。

【請求項5】 ネットワークを介して他の情報処理装置と接続される情報処理装置を制御するプログラムであって、

オンオフの入力を制御する入力制御手段と、前記入力制御ステップの処理でオンが入力された第1の

タイミングの計測を制御する第1のタイミング計測制御ステップと、

前記入力制御ステップの処理でオフが入力された第2のタイミングの計測を制御する第2のタイミング計測制御ステップと、

前記第1のタイミング、および、前記第2のタイミングの前記ネットワークを介した他の情報処理装置への送信を制御する送信制御ステップとを含むことを特徴とする

コンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項6】 ネットワークを介して他の情報処理装置と接続される情報処理装置を制御するコンピュータに、オンオフの入力を制御する入力制御手段と、

前記入力制御ステップの処理でオンが入力された第1のタイミングの計測を制御する第1のタイミング計測制御

ステップと、

前記入力制御ステップの処理でオフが入力された第2のタイミングの計測を制御する第2のタイミング計測制御

ステップと、

前記第1のタイミング、および、前記第2のタイミングの前記ネットワークを介した他の情報処理装置への送信を制御する送信制御ステップとを実行させるプログラ

ム。

【請求項7】 ネットワークを介して他の情報処理装置と接続される情報処理装置において、

オンオフを入力する入力手段と、

前記入力手段によりオンが入力された第1のタイミングを計測する第1のタイミング計測手段と、

前記入力手段によりオフが入力された第2のタイミングを計測する第2のタイミング計測手段と、

前記他の情報処理装置より送信されてくる、前記他の情報処理装置の他の入力手段によりオンが入力された第3の

タイミング、および、オフが入力された第4のタイミングを受信する受信手段と、

前記第1のタイミングと前記第3のタイミング、および、前記第2のタイミングと前記第4のタイミングを、

それぞれ比較する比較手段と、

前記比較手段の比較結果に基づいて、前記他の情報処理装置との認証処理を実行する認証手段とを備えることを

特徴とする情報処理装置。

【請求項8】 前記ネットワークは、ブルートゥースにより構成されることを特徴とする請求項7に記載の情報処理装置。

【請求項9】 前記比較手段は、前記第1のタイミングと前記第3のタイミング、および、前記第2のタイミン

グと第4のタイミングとの、それぞれの差を求めて、前記差が所定範囲内であるか否かを比較することを特徴と

する請求項7に記載の情報処理装置。

【請求項10】 前記認証手段は、前記それぞれの差が、いずれも前記所定の範囲内であるとき、前記他の情

報処理装置を認証することを特徴とする請求項9に記載の情報処理装置。

【請求項11】 前記第1のタイミング計測手段、および、前記第2のタイミング計測手段は、いずれも複数回

数のタイミングを計測し、前記受信手段は、前記他の入力手段により複数回数オンが入力された第3のタイ

ミング、および、複数回数オフにされた第4のタイミングを受信することを特徴とする請求項7に記載の情報処理装

置。

【請求項12】 ネットワークを介して他の情報処理装置と接続される情報処理装置の情報処理方法において、

オンオフを入力する入力ステップと、前記入力ステップの処理でオンが入力された第1のタイ

ミングを計測する第1のタイミング計測ステップと、前記入力ステップの処理でオフが入力された第2のタイ

ミングを計測する第2のタイミング計測ステップと、前記他の情報処理装置より送信されてくる、前記他の情報処理装置の他の入力ステップの処理でオンが入力された第3のタイミング、および、オフが入力された第4のタイミングを受信する受信手段と、前記第1のタイミングと前記第3のタイミング、および、前記第2のタイミングと前記第4のタイミングを、それぞれ比較する比較ステップと、前記比較ステップの処理での比較結果に基づいて、前記他の情報処理装置との認証処理を実行する認証ステップとを含むことを特徴とする情報処理方法。

【請求項13】 ネットワークを介して他の情報処理装置と接続される情報処理装置を制御するプログラムであって、オンオフの入力を制御する入力ステップと、前記入力制御ステップの処理でオンが入力された第1のタイミングの計測を制御する第1のタイミング計測制御ステップと、前記入力制御ステップの処理でオフが入力された第2のタイミングの計測を制御する第2のタイミング計測制御ステップと、前記他の情報処理装置より送信されてくる、前記他の情報処理装置の他の入力制御ステップの処理でオンが入力された第3のタイミング、および、オフが入力された第4のタイミングの受信を制御する受信制御手段と、前記第1のタイミングと前記第3のタイミング、および、前記第2のタイミングと前記第4のタイミングの、それぞれの比較を制御する比較制御ステップと、前記比較制御ステップの処理での比較結果に基づいて、前記他の情報処理装置との認証処理の実行を制御する認証制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項14】 ネットワークを介して他の情報処理装置と接続される情報処理装置を制御するコンピュータに、オンオフの入力を制御する入力ステップと、前記入力制御ステップの処理でオンが入力された第1のタイミングの計測を制御する第1のタイミング計測制御ステップと、前記入力制御ステップの処理でオフが入力された第2のタイミングの計測を制御する第2のタイミング計測制御ステップと、前記他の情報処理装置より送信されてくる、前記他の情報処理装置の他の入力制御ステップの処理でオンが入力された第3のタイミング、および、オフが入力された第4のタイミングの受信を制御する受信制御手段と、前記第1のタイミングと前記第3のタイミング、および、前記第2のタイミングと前記第4のタイミングの、それぞれの比較を制御する比較制御ステップと、前記比較制御ステップの処理での比較結果に基づいて、前記他

の情報処理装置との認証処理の実行を制御する認証制御ステップとを実行させるプログラム。

【請求項15】 ネットワークを介して相互に接続される第1の情報処理装置と第2の情報処理装置からなる情報処理システムにおいて、第1の情報処理装置は、オンオフを入力する第1の入力手段と、前記第1の入力手段によりオンが入力された第1のタイミングを計測する第1のタイミング計測手段と、前記第1の入力手段によりオフが入力された第2のタイミングを計測する第2のタイミング計測手段と、前記第1のタイミング、および、前記第2のタイミングを前記ネットワークを介して前記第2の情報処理装置に送信する送信手段とを備え、第2の情報処理装置は、オンオフを入力する第2の入力手段と、前記第2の入力手段によりオンが入力されたタイミングを計測する第3のタイミング計測手段と、前記第2の入力手段によりオフが入力されたタイミングを計測する第4のタイミング計測手段と、前記第1の情報処理装置より送信されてくる、前記第1のタイミング、および、前記第2のタイミングを受信する受信手段と、前記第1のタイミングと前記第3のタイミング、および、前記第2のタイミングと前記第4のタイミングとをそれぞれ比較する比較手段と、前記比較手段の比較結果に基づいて、前記第1の情報処理装置との認証処理を実行する認証手段とを備えることを特徴とする情報処理システム。

【請求項16】 ネットワークを介して相互に接続される第1の情報処理装置と第2の情報処理装置からなる情報処理システムの情報処理方法において、第1の情報処理装置の情報処理方法は、オンオフを入力する第1の入力ステップと、前記第1の入力ステップの処理でオンが入力された第1のタイミングを計測する第1のタイミング計測ステップと、前記第1の入力ステップの処理でオフが入力された第2のタイミングを計測する第2のタイミング計測ステップと、前記第1のタイミング、および、前記第2のタイミングを前記ネットワークを介して前記第2の情報処理装置に送信する送信ステップとを含み、第2の情報処理装置の情報処理方法は、オンオフを入力する第2の入力ステップと、前記第2の入力ステップの処理でオンが入力されたタイミングを計測する第3のタイミング計測ステップと、前記第2の入力ステップの処理でオフが入力されたタイミングを計測する第4のタイミング計測ステップと、前記第1の情報処理装置より送信されてくる、前記第1

のタイミング、および、前記第2のタイミングを受信する受信ステップと、

前記第1のタイミングと前記第3のタイミング、および、前記第2のタイミングと前記第4のタイミングとをそれぞれ比較する比較ステップと、

前記比較ステップの処理での比較結果に基づいて、前記第1の情報処理装置との認証処理を実行する認証ステップとを含むことを特徴とする情報処理システムの情報処理方法。

【請求項17】 ネットワークを介して相互に接続される第1の情報処理装置と第2の情報処理装置からなる情報処理システムを制御するプログラムであって、

第1の情報処理装置を制御するプログラムは、オンオフの入力を制御する第1の入力制御ステップと、前記第1の入力制御ステップの処理でオンが入力された第1のタイミングの計測を制御する第1のタイミング計測制御ステップと、

前記第1の入力制御ステップの処理でオフが入力された第2のタイミングの計測を制御する第2のタイミング計測制御ステップと、

前記第1のタイミング、および、前記第2のタイミングの前記ネットワークを介した前記第2の情報処理装置への送信を制御する送信制御ステップとを含み、

第2の情報処理装置を制御するプログラムは、オンオフの入力を制御する第2の入力制御ステップと、前記第2の入力制御ステップの処理でオンが入力されたタイミングの計測を制御する第3のタイミング計測制御ステップと、

前記第2の入力制御ステップの処理でオフが入力されたタイミングの計測を制御する第4のタイミング計測制御ステップと、

前記第1の情報処理装置より送信されてくる、前記第1のタイミング、および、前記第2のタイミングの受信を制御する受信制御ステップと、

前記第1のタイミングと前記第3のタイミング、および、前記第2のタイミングと前記第4のタイミングとのそれぞれの比較を制御する比較制御ステップと、

前記比較制御ステップの処理での比較結果に基づいて、前記第1の情報処理装置との認証処理の実行を制御する認証制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項18】 ネットワークを介して相互に接続される第1の情報処理装置と第2の情報処理装置からなる情報処理システムを制御するコンピュータのうち、第1の情報処理装置を制御するコンピュータに、オンオフの入力を制御する第1の入力制御ステップと、前記第1の入力制御ステップの処理でオンが入力された第1のタイミングの計測を制御する第1のタイミング計測制御ステップと、

前記第1の入力制御ステップの処理でオフが入力された第2のタイミングの計測を制御する第2のタイミング計測制御ステップと、

前記第1のタイミング、および、前記第2のタイミングの前記ネットワークを介した前記第2の情報処理装置への送信を制御する送信制御ステップとを実行させ、

第2の情報処理装置を制御するコンピュータに、オンオフの入力を制御する第2の入力制御ステップと、前記第2の入力制御ステップの処理でオンが入力されたタイミングの計測を制御する第3のタイミング計測制御ステップと、

前記第2の入力制御ステップの処理でオフが入力されたタイミングの計測を制御する第4のタイミング計測制御ステップと、

前記第1の情報処理装置より送信されてくる、前記第1のタイミング、および、前記第2のタイミングの受信を制御する受信制御ステップと、

前記第1のタイミングと前記第3のタイミング、および、前記第2のタイミングと前記第4のタイミングとのそれぞれの比較を制御する比較制御ステップと、

前記比較制御ステップの処理での比較結果に基づいて、前記第1の情報処理装置との認証処理の実行を制御する認証制御ステップとを実行させるプログラム。

【請求項19】 ネットワークを介して他の情報処理装置と接続される情報処理装置において、

オンオフを入力する入力手段と、

前記入力手段によりオンが入力された第1のタイミングを計測する第1のタイミング計測手段と、

前記入力手段によりオフが入力された第2のタイミングを計測する第2のタイミング計測手段と、

前記第1のタイミング、または、前記第2のタイミングを前記ネットワークを介して前記他の情報処理装置に送信する送信手段と、

前記他の情報処理装置より送信されてくる、前記送信手段により送信された前記第1のタイミング、または、前記第2のタイミングのいずれかに対応した、前記他の情報処理装置の他の入力手段によりオンが入力された第3のタイミング、または、オフが入力された第4のタイミングを受信する受信手段と、

前記第1のタイミングと前記第3のタイミング、または、前記第2のタイミングと前記第4のタイミングとを比較する比較手段と、

前記比較手段の比較結果に基づいて、前記他の情報処理装置との認証処理を実行する認証手段とを備えることを特徴とする情報処理装置。

【請求項20】 前記ネットワークは、ブルートゥースにより構成されることを特徴とする請求項19に記載の情報処理装置。

【請求項21】 前記第1のタイミング計測手段、および、前記第2のタイミング計測手段は、いずれも複数回

数のタイミングを計測し、前記受信手段は、前記他の入力手段により複数回数オンが入力された第3のタイミング、および、複数回数オフにされた第4のタイミングを受信することを特徴とする請求項19に記載の情報処理装置。

【請求項22】 前記比較手段は、前記第1のタイミングと前記第3のタイミング、または、前記第2のタイミングと前記第4のタイミングとの差を求めて、前記差が所定範囲内になるか否かを比較することを特徴とする請求項19に記載の情報処理装置。

【請求項23】 前記認証手段は、前記差が、前記所定の範囲内であるとき、前記他の情報処理装置を認証することを特徴とする請求項22に記載の情報処理装置。

【請求項24】 ネットワークを介して他の情報処理装置と接続される情報処理装置の情報処理方法において、オンオフを入力する入力ステップと、前記入力ステップの処理でオンが入力された第1のタイミングを計測する第1のタイミング計測ステップと、前記入力ステップの処理でオフが入力された第2のタイミングを計測する第2のタイミング計測ステップと、前記第1のタイミング、または、前記第2のタイミングを前記ネットワークを介して前記他の情報処理装置に送信する送信ステップと、前記他の情報処理装置より送信されてくる、前記送信ステップの処理で送信された前記第1のタイミング、または、前記第2のタイミングのいずれかに対応した、前記他の情報処理装置の他の入力ステップの処理でオンが入力された第3のタイミング、または、オフが入力された第4のタイミングを受信する受信ステップと、前記第1のタイミングと前記第3のタイミング、または、前記第2のタイミングと前記第4のタイミングとを比較する比較ステップと、前記比較ステップの処理での比較結果に基づいて、前記他の情報処理装置との認証処理を実行する認証ステップとを含むことを特徴とする情報処理方法。

【請求項25】 ネットワークを介して他の情報処理装置と接続される情報処理装置を制御するプログラムであって、オンオフの入力を制御する入力制御ステップと、前記入力制御ステップの処理でオンが入力された第1のタイミングの計測を制御する第1のタイミング計測制御ステップと、前記入力制御ステップの処理でオフが入力された第2のタイミングの計測を制御する第2のタイミング計測制御ステップと、前記第1のタイミング、または、前記第2のタイミングの前記ネットワークを介した前記他の情報処理装置への送信を制御する送信制御ステップと、前記他の情報処理装置より送信されてくる、前記送信制御ステップの処理で送信された前記第1のタイミング、

または、前記第2のタイミングのいずれかに対応した、前記他の情報処理装置の他の入力制御ステップの処理でオンが入力された第3のタイミング、または、オフが入力された第4のタイミングの受信を制御する受信制御ステップと、

前記第1のタイミングと前記第3のタイミング、または、前記第2のタイミングと前記第4のタイミングとの比較を制御する比較制御ステップと、前記比較制御ステップの処理での比較結果に基づいて、前記他の情報処理装置との認証処理の実行を制御する認証制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項26】 ネットワークを介して他の情報処理装置と接続される情報処理装置を制御するコンピュータに、オンオフの入力を制御する入力制御ステップと、前記入力制御ステップの処理でオンが入力された第1のタイミングの計測を制御する第1のタイミング計測制御ステップと、前記入力制御ステップの処理でオフが入力された第2のタイミングの計測を制御する第2のタイミング計測制御ステップと、前記第1のタイミング、または、前記第2のタイミングの前記ネットワークを介した前記他の情報処理装置への送信を制御する送信制御ステップと、前記他の情報処理装置より送信されてくる、前記送信制御ステップの処理で送信された前記第1のタイミング、または、前記第2のタイミングのいずれかに対応した、前記他の情報処理装置の他の入力制御ステップの処理でオンが入力された第3のタイミング、または、オフが入力された第4のタイミングの受信を制御する受信制御ステップと、前記第1のタイミングと前記第3のタイミング、または、前記第2のタイミングと前記第4のタイミングとの比較を制御する比較制御ステップと、前記比較制御ステップの処理での比較結果に基づいて、前記他の情報処理装置との認証処理の実行を制御する認証制御ステップとを実行させるプログラム。

【請求項27】 ネットワークを介して相互に接続される、オンオフを入力する第1の入力手段と、前記第1の入力手段によりオンが入力された第1のタイミングを計測する第1のタイミング計測手段と、前記第1の入力手段によりオフが入力された第2のタイミングを計測する第2のタイミング計測手段と、前記第2のタイミングを前記ネットワークを介して第2の情報処理装置に送信する第1の送信手段とを備えた第1の情報処理装置と、オンオフを入力する第2の入力手段と、前記第2の入力手段によりオンが入力された第3のタイミングを計測する第3のタイミング計測手段と前記第2の入力手段により

オフが入力された第4のタイミングを計測する第4のタイミング計測手段と、前記第3のタイミングを前記ネットワークを介して第1の情報処理装置に送信する第2の送信手段とを備えた前記第2の情報処理装置から構成された情報処理システムにおいて、

前記第1の情報処理装置は、  
前記第2の情報処理装置より送信されてくる、前記第3のタイミングを受信する第1の受信手段と、  
前記第1のタイミングと前記第3のタイミングを比較する第1の比較手段と、  
前記第1の比較手段の比較結果に基づいて、前記第2の情報処理装置との認証処理を実行する第1の認証手段とを備え、

前記第2の情報処理装置は、  
前記第1の情報処理装置より送信されてくる、前記第2のタイミングを受信する第2の受信手段と、  
前記第2のタイミングと前記第4のタイミングを比較する第2の比較手段と、  
前記第2の比較手段の比較結果に基づいて、前記第1の情報処理装置との認証処理を実行する第2の認証手段とを備えることを特徴とする情報処理システム。

【請求項28】 ネットワークを介して相互に接続される、オンオフを入力する第1の入力手段と、前記第1の入力手段によりオンが入力された第1のタイミングを計測する第1のタイミング計測手段と、前記第1の入力手段によりオフが入力された第2のタイミングを計測する第2のタイミング計測手段と、前記第2のタイミングを前記ネットワークを介して第2の情報処理装置に送信する第1の送信手段とを備えた第1の情報処理装置と、オンオフを入力する第2の入力手段と、前記第2の入力手段によりオンが入力された第3のタイミングを計測する第3のタイミング計測手段と前記第2の入力手段によりオフが入力された第4のタイミングを計測する第4のタイミング計測手段と、前記第3のタイミングを前記ネットワークを介して第1の情報処理装置に送信する第2の送信手段とを備えた前記第2の情報処理装置から構成された情報処理システムの情報処理方法において、  
前記第1の情報処理装置の情報処理方法は、  
前記第2の情報処理装置より送信されてくる、前記第3のタイミングを受信する第1の受信ステップと、  
前記第1のタイミングと前記第3のタイミングを比較する第1の比較ステップと、  
前記第1の比較ステップの処理での比較結果に基づいて、前記第2の情報処理装置との認証処理を実行する第1の認証ステップとを含み、  
前記第2の情報処理装置の情報処理方法は、  
前記第1の情報処理装置より送信されてくる、前記第2のタイミングを受信する第2の受信ステップと、  
前記第2のタイミングと前記第4のタイミングを比較する第2の比較ステップと、

前記第2の比較ステップの処理での比較結果に基づいて、前記第1の情報処理装置との認証処理を実行する第2の認証ステップとを含むことを特徴とする情報処理システムの情報処理方法。

【請求項29】 ネットワークを介して相互に接続される、オンオフを入力する第1の入力手段と、前記第1の入力手段によりオンが入力された第1のタイミングを計測する第1のタイミング計測手段と、前記第1の入力手段によりオフが入力された第2のタイミングを計測する第2のタイミング計測手段と、前記第2のタイミングを前記ネットワークを介して第2の情報処理装置に送信する第1の送信手段とを備えた第1の情報処理装置と、オンオフを入力する第2の入力手段と、前記第2の入力手段によりオンが入力された第3のタイミングを計測する第3のタイミング計測手段と前記第2の入力手段によりオフが入力された第4のタイミングを計測する第4のタイミング計測手段と、前記第3のタイミングを前記ネットワークを介して第1の情報処理装置に送信する第2の送信手段とを備えた第2の情報処理装置から構成された情報処理システムを制御するプログラムであって、  
前記第1の情報処理装置を制御するプログラムは、  
前記第2の情報処理装置より送信されてくる、前記第3のタイミングの受信を制御する第1の受信制御ステップと、  
前記第1のタイミングと前記第3のタイミングとの比較を制御する第1の比較制御ステップと、  
前記第1の比較制御ステップの処理での比較結果に基づいて、前記第2の情報処理装置との認証処理の実行を制御する第1の認証制御ステップとを含み、  
前記第2の情報処理装置を制御するプログラムは、  
前記第1の情報処理装置より送信されてくる、前記第2のタイミングの受信を制御する第2の受信制御ステップと、  
前記第2のタイミングと前記第4のタイミングとの比較を制御する第2の比較制御ステップと、  
前記第2の比較制御ステップの処理での比較結果に基づいて、前記第1の情報処理装置との認証処理の実行を制御する第2の認証制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

【請求項30】 ネットワークを介して相互に接続される、オンオフを入力する第1の入力手段と、前記第1の入力手段によりオンが入力された第1のタイミングを計測する第1のタイミング計測手段と、前記第1の入力手段によりオフが入力された第2のタイミングを計測する第2のタイミング計測手段と、前記第2のタイミングを前記ネットワークを介して第2の情報処理装置に送信する第1の送信手段とを備えた第1の情報処理装置と、オンオフを入力する第2の入力手段と、前記第2の入力手段によりオンが入力された第3のタイミングを計測する

第3のタイミング計測手段と前記第2の入力手段によりオフが入力された第4のタイミングを計測する第4のタイミング計測手段と、前記第3のタイミングを前記ネットワークを介して第1の情報処理装置に送信する第2の送信手段とを備えた第2の情報処理装置から構成された情報処理システムを制御するコンピュータのうち、前記第1の情報処理装置を制御するコンピュータに、前記第2の情報処理装置より送信されてくる、前記第3のタイミングの受信を制御する第1の受信制御ステップと、前記第1のタイミングと前記第3のタイミングとの比較を制御する第1の比較制御ステップと、前記第1の比較制御ステップの処理での比較結果に基づいて、前記第2の情報処理装置との認証処理の実行を制御する第1の認証制御ステップとを実行させ、前記第2の情報処理装置を制御するコンピュータに、前記第1の情報処理装置より送信されてくる、前記第2のタイミングの受信を制御する第2の受信制御ステップと、前記第2のタイミングと前記第4のタイミングとの比較を制御する第2の比較制御ステップと、前記第2の比較制御ステップの処理での比較結果に基づいて、前記第1の情報処理装置との認証処理の実行を制御する第2の認証制御ステップとを実行させるプログラム。

#### 【発明の詳細な説明】

##### 【0001】

【発明の属する技術分野】本発明は、情報処理装置および方法、情報処理システム、記録媒体、並びにプログラムに関し、特に、簡易に電子機器間の相互認証処理を実行できるようにした情報処理装置および方法、記録媒体、情報処理システム、並びにプログラムに関する。

##### 【0002】

【従来の技術】ブルートゥースを利用した至近距離での電子機器間の無線通信技術が一般に普及しつつある。

【0003】ブルートゥースは、2.45GHzの周波数帯域を利用した無線通信技術で、到達距離は最大約10m程度のものである。類似した通信方法として赤外線通信があるが、ブルートゥースの場合は無線通信であるため障害物を通して通信することが可能であり、その点が、赤外線通信と異なり、メリットとなっている。

【0004】ブルートゥースにより、例えば、図1に示すように、パーソナルコンピュータ(PC: Personal Computer)1とカムコード2(図1(A))、携帯電話機3とハンディカムコード4(図1(B))、カムコード2と携帯情報端末機5(図1(C))、および、携帯型パーソナルコンピュータ6と携帯情報通信端末機5(図1(D))などの間で、無線通信による情報の授受が可能とされる。

【0005】このように特に配線を必要としないブルー

トゥースの無線接続により、例えば、携帯情報端末機5のデータを異なる部屋に存在する携帯型パーソナルコンピュータ6に転送したり、携帯電話機3をユーザの衣服のポケットに入れたままハンディカムコード4と接続し、ハンディカムコード4に記録されている映像をインターネットを介して他の電子機器に送信するということも可能である。

【0006】これらの電子機器間での通信を行うためには、通信による誤動作、誤接続、または、データ転送時のデータの漏洩などを防止するため、それぞれの電子機器間で、1回目の通信で相互認証処理を実行させる。このとき、ユーザは必要に応じて、英数字などからなるパスワードの入力を、それぞれの電子機器で行い、認証処理を実行させる。

【0007】ここで、例えば、図1(A)で示す、パーソナルコンピュータ1とカムコード2の間で最初に行われる認証処理について、図2のフローチャートを参照して説明する。

【0008】ステップS1において、パーソナルコンピュータ1(以下においては、PC1とも称する)は、キーボードなどの入力部より、ブルートゥースの規格上でPIN(Personal Identification Number)と呼ばれるユーザを特定するパスワードが入力されたか否かを判定し、入力されるまでその処理を繰り返し、入力されたと判定された場合、その処理は、ステップS2に進む。このとき、カムコード2も、ステップS21において、同様の処理を実行する。

【0009】ステップS2において、PC1は、乱数R0を発生しカムコード2に送信し、ステップS3において、乱数R0、PIN、および、BDADDR-Cam(Blue-tooth Device Address for Camcorder: カムコード2を識別する固有の番号)から所定の関数E22により共通鍵E22(R0, PIN, BDADDR-Cam)を演算する。ここで、BDADDR-Camは、ユーザがPC1と接続しようとする電子機器(今の場合、カムコード2)を指定することで選択される。

【0010】ステップS22において、カムコード2は、ステップS3の処理でPC1が使用したものと同様の関数E22により、乱数R0、PIN、および、BDADDR-Camから共通鍵CK(=E22(R0, PIN, BDADDR-Cam))を演算し、PC1の応答として送信する。

【0011】ステップS4において、PC1は、認証用の乱数R1を発生し、カムコード2に送信すると共に、ステップS5において、乱数R1、共通鍵CK、および、BDADDR-Camより、関数E1を用いてパスワードA(=E1(R1, CK, BDADDR-Cam))を演算する。

【0012】このとき、ステップS23において、カムコード2は、PC1より送信されてきた乱数R1、共通鍵、および、BDADDR-Camより、ステップS4の処理でPC1により使用されたものと同様の関数E1によりパスワードA'(=E1(R1, CK, BDADDR-Cam))を演算し、PC1に送信す

る。

【0013】ステップS6において、PC1は、自らが演算したパスワードAと、カムコード2より送信されてきたパスワードA'が一致するか否かを判定し、一致したと判定した場合、ステップS7において、パスワードが一致したことをカムコード2に通知する。

【0014】ステップS24において、カムコード2は、PC1からの通知を受信し、ステップS25において、パスワードAとパスワードA'が一致したか否かを判定する。今の場合、ステップS7の処理によりパスワードが一致している通知がPC1より送信されてきているので、ステップS26において、認証用の乱数R2を発生し、PC1に送信すると共に、ステップS27において、乱数R2、共通鍵CK、および、BDADDR-PCより、認証用の関数パスワードB(=E1(R2, CK, BDADDR-PC))を生成する。一方、ステップS8において、PC1は、カムコード2より送信されてきた乱数R2、共通鍵CK、および、BDADDR-PCより、関数E1を使用してパスワードB'(=E1(R2, CK, BDADDR-PC))を演算し、カムコード2に送信する。

【0015】ステップS28において、カムコード2は、パスワードBとパスワードB'が一致したか否かを判定し、一致したと判定した場合、その処理は、ステップS29において、認証が認められたことを認識し、同時に、パスワードBとパスワードB'が一致したことをPC1に送信する。ステップS9において、PC1は、通知を受信し、パスワードが一致し、認証が認められたことが認識する。

【0016】ステップS6において、パスワードAとパスワードA'が一致しないと判定された場合、ステップS10において、パスワードAとパスワードA'が一致しなかったことをカムコード2に通知し、その処理を終了する。

【0017】この場合、ステップS24では、パスワードAとパスワードA'が一致しなかったことを示す通知が、カムコード2に受信されるので、ステップS25において、カムコード2は、パスワードAとパスワードA'が一致しなかったと判定し、その処理は、終了する。

【0018】ステップS28において、パスワードBとパスワードB'が一致しないと判定された場合、ステップS30において、カムコード2は、認証が認められないことを認識し、パスワードBとパスワードB'が一致しなかったことを示す通知をPC1に送信する。

【0019】そして、2回目以降の接続では、通信させようとする電子機器が、1回目の認証処理で記憶されたパスワードA,Bや、最初の接続で生成された共通鍵CKなどを利用して自動認証を行うことにより、ユーザによるパスワードの入力処理が省略されるようになっている。

【0020】

【発明が解決しようとする課題】しかしながら、上記のような構成では、PC1とカムコード2や、LAN(Local A

rea Network)内の無線アクセスポイントに接続するなど、固定的な通信相手に対して行う場合、あまり問題とされないが、例えば、PC1上で実行させるアプリケーションソフトウェアなどにより他の電子機器と一時的に画像データなどを交換し、次のタイミングでは、通信相手を変えるような場合、新しい接続相手となる他の電子機器と接続する度に、毎回パスワードの入力が必要となるため、その処理が面倒なものであったと言う課題があった。

【0021】本発明はこのような状況に鑑みてなされたものであり、ブルートゥースによる無線通信を実行する際、最初の相互認証を簡易な処理で実行できるようにするものである。

【0022】

【課題を解決するための手段】本発明の第1の情報処理装置は、オンオフを入力する入力手段と、入力手段によりオンが入力された第1のタイミングを計測する第1のタイミング計測手段と、入力手段によりオフが入力された第2のタイミングを計測する第2のタイミング計測手段と、第1のタイミング、および、第2のタイミングをネットワークを介して他の情報処理装置に送信する送信手段とを備えることを特徴とする。

【0023】前記ネットワークは、ブルートゥースにより構成されるようにすることができる。

【0024】前記第1のタイミング計測手段、および、第2のタイミング計測手段には、いずれも複数回数のタイミングを計測させるようにすることができる。

【0025】本発明の第1の情報処理方法は、オンオフを入力する入力手段と、入力ステップの処理でオンが入力された第1のタイミングを計測する第1のタイミング計測ステップと、入力ステップの処理でオフが入力された第2のタイミングを計測する第2のタイミング計測ステップと、第1のタイミング、および、第2のタイミングをネットワークを介して他の情報処理装置に送信する送信ステップとを含むことを特徴とする。

【0026】第1の記録媒体のプログラムは、オンオフの入力を制御する入力制御手段と、入力制御ステップの処理でオンが入力された第1のタイミングの計測を制御する第1のタイミング計測制御ステップと、入力制御ステップの処理でオフが入力された第2のタイミングの計測を制御する第2のタイミング計測制御ステップと、第1のタイミング、および、第2のタイミングのネットワークを介した他の情報処理装置への送信を制御する送信制御ステップとを含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている。

【0027】本発明の第1のプログラムは、オンオフの入力を制御する入力制御手段と、入力制御ステップの処理でオンが入力された第1のタイミングの計測を制御する第1のタイミング計測制御ステップと、入力制御ステップの処理でオフが入力された第2のタイミングの計測



を制御する第2のタイミング計測制御ステップと、第1のタイミング、および、第2のタイミングのネットワークを介した他の情報処理装置への送信を制御する送信制御ステップとを実行させる。

【0028】本発明の第2の情報処理装置は、オンオフを入力する入力手段と、入力手段によりオンが入力された第1のタイミングを計測する第1のタイミング計測手段と、入力手段によりオフが入力された第2のタイミングを計測する第2のタイミング計測手段と、他の情報処理装置より送信されてくる、他の情報処理装置の他の入力手段によりオンが入力された第3のタイミング、および、オフが入力された第4のタイミングを受信する受信手段と、第1のタイミングと第3のタイミング、および、第2のタイミングと第4のタイミングを、それぞれ比較する比較手段と、比較手段の比較結果に基づいて、他の情報処理装置との認証処理を実行する認証手段とを備えることを特徴とする。

【0029】前記ネットワークは、ブルートゥースにより構成されるようにすることができる。

【0030】前記比較手段には、第1のタイミングと第3のタイミング、および、第2のタイミングと第4のタイミングとの、それぞれの差を求めて、差が所定範囲内であるか否かを比較させるようにすることができる。

【0031】前記認証手段には、それぞれの差が、いずれも所定の範囲内であるとき、他の情報処理装置を認証させるようにすることができる。

【0032】前記第1のタイミング計測手段、および、第2のタイミング計測手段には、いずれも複数回のタイミングを計測させ、受信手段には、他の入力手段により複数回数オンが入力された第3のタイミング、および、複数回数オフにされた第4のタイミングを受信させるようにする。

【0033】本発明の第2の情報処理方法は、オンオフを入力する入力ステップと、入力ステップの処理でオンが入力された第1のタイミングを計測する第1のタイミング計測ステップと、入力ステップの処理でオフが入力された第2のタイミングを計測する第2のタイミング計測ステップと、他の情報処理装置より送信されてくる、他の情報処理装置の他の入力ステップの処理でオンが入力された第3のタイミング、および、オフが入力された第4のタイミングを受信する受信手段と、第1のタイミングと第3のタイミング、および、第2のタイミングと第4のタイミングを、それぞれ比較する比較ステップと、比較ステップの処理での比較結果に基づいて、他の情報処理装置との認証処理を実行する認証ステップとを含むことを特徴とする。

【0034】本発明の第2の記録媒体のプログラムは、オンオフの入力を制御する入力ステップと、入力制御ステップの処理でオンが入力された第1のタイミングの計測を制御する第1のタイミング計測制御ステップと、入

力制御ステップの処理でオフが入力された第2のタイミングの計測を制御する第2のタイミング計測制御ステップと、他の情報処理装置より送信されてくる、他の情報処理装置の他の入力制御ステップの処理でオンが入力された第3のタイミング、および、オフが入力された第4のタイミングの受信を制御する受信制御手段と、第1のタイミングと第3のタイミング、および、第2のタイミングと第4のタイミングの、それぞれの比較を制御する比較制御ステップと、比較制御ステップの処理での比較結果に基づいて、他の情報処理装置との認証処理の実行を制御する認証制御ステップとを含むことを特徴とする。

【0035】本発明の第2のプログラムは、オンオフの入力を制御する入力ステップと、入力制御ステップの処理でオンが入力された第1のタイミングの計測を制御する第1のタイミング計測制御ステップと、入力制御ステップの処理でオフが入力された第2のタイミングの計測を制御する第2のタイミング計測制御ステップと、他の情報処理装置より送信されてくる、他の情報処理装置の他の入力制御ステップの処理でオンが入力された第3のタイミング、および、オフが入力された第4のタイミングの受信を制御する受信制御手段と、第1のタイミングと第3のタイミング、および、第2のタイミングと第4のタイミングの、それぞれの比較を制御する比較制御ステップと、比較制御ステップの処理での比較結果に基づいて、他の情報処理装置との認証処理の実行を制御する認証制御ステップとを実行させる。

【0036】本発明の第1の情報処理システムは、第1の情報処理装置が、オンオフを入力する第1の入力手段と、第1の入力手段によりオンが入力された第1のタイミングを計測する第1のタイミング計測手段と、第1の入力手段によりオフが入力された第2のタイミングを計測する第2のタイミング計測手段と、第1のタイミング、および、第2のタイミングをネットワークを介して第2の情報処理装置に送信する送信手段とを備え、第2の情報処理装置が、オンオフを入力する第2の入力手段と、第2の入力手段によりオンが入力されたタイミングを計測する第3のタイミング計測手段と、第2の入力手段によりオフが入力されたタイミングを計測する第4のタイミング計測手段と、第1の情報処理装置より送信されてくる、第1のタイミング、および、第2のタイミングを受信する受信手段と、第1のタイミングと第3のタイミング、および、第2のタイミングと第4のタイミングとをそれぞれ比較する比較手段と、比較手段の比較結果に基づいて、第1の情報処理装置との認証処理を実行する認証手段とを備えることを特徴とする。

【0037】本発明の第1の情報処理システムの情報処理方法は、第1の情報処理装置の情報処理方法が、オンオフを入力する第1の入力ステップと、第1の入力ステップの処理でオンが入力された第1のタイミングを計測

する第1のタイミング計測ステップと、第1の入力ステップの処理でオフが入力された第2のタイミングを計測する第2のタイミング計測ステップと、第1のタイミング、および、第2のタイミングをネットワークを介して第2の情報処理装置に送信する送信ステップとを含み、第2の情報処理装置の情報処理方法は、オンオフを入力する第2の入力ステップと、第2の入力ステップの処理でオンが入力されたタイミングを計測する第3のタイミング計測ステップと、第2の入力ステップの処理でオフが入力されたタイミングを計測する第4のタイミング計測ステップと、第1の情報処理装置より送信されてくる、第1のタイミング、および、第2のタイミングを受信する受信ステップと、第1のタイミングと第3のタイミング、および、第2のタイミングと第4のタイミングとをそれぞれ比較する比較ステップと、比較ステップの処理での比較結果に基づいて、第1の情報処理装置との認証処理を実行する認証ステップとを含むことを特徴とする。

【0038】本発明の第3の記録媒体のプログラムは、第1の情報処理装置を制御するプログラムが、オンオフの入力を制御する第1の入力制御ステップと、第1の入力制御ステップの処理でオンが入力された第1のタイミングの計測を制御する第1のタイミング計測制御ステップと、第1の入力制御ステップの処理でオフが入力された第2のタイミングの計測を制御する第2のタイミング計測制御ステップと、第1のタイミング、および、第2のタイミングのネットワークを介した第2の情報処理装置への送信を制御する送信制御ステップとを含み、第2の情報処理装置を制御するプログラムが、オンオフの入力を制御する第2の入力制御ステップと、第2の入力制御ステップの処理でオンが入力されたタイミングの計測を制御する第3のタイミング計測制御ステップと、第2の入力制御ステップの処理でオフが入力されたタイミングの計測を制御する第4のタイミング計測制御ステップと、第1の情報処理装置より送信されてくる、第1のタイミング、および、第2のタイミングの受信を制御する受信制御ステップと、第1のタイミングと第3のタイミング、および、第2のタイミングと第4のタイミングとのそれぞれの比較を制御する比較制御ステップと、比較制御ステップの処理での比較結果に基づいて、第1の情報処理装置との認証処理の実行を制御する認証制御ステップとを含むことを特徴とする。

【0039】本発明の第3のプログラムは、第1の情報処理装置を制御するコンピュータに、オンオフの入力を制御する第1の入力制御ステップと、第1の入力制御ステップの処理でオンが入力された第1のタイミングの計測を制御する第1のタイミング計測制御ステップと、第1の入力制御ステップの処理でオフが入力された第2のタイミングの計測を制御する第2のタイミング計測制御ステップと、第1のタイミング、および、第2のタイミ

ングのネットワークを介した第2の情報処理装置への送信を制御する送信制御ステップとを実行させ、第2の情報処理装置を制御するコンピュータに、オンオフの入力を制御する第2の入力制御ステップと、第2の入力制御ステップの処理でオンが入力されたタイミングの計測を制御する第3のタイミング計測制御ステップと、第2の入力制御ステップの処理でオフが入力されたタイミングの計測を制御する第4のタイミング計測制御ステップと、第1の情報処理装置より送信されてくる、第1のタイミング、および、第2のタイミングの受信を制御する受信制御ステップと、第1のタイミングと第3のタイミング、および、第2のタイミングと第4のタイミングとのそれぞれの比較を制御する比較制御ステップと、比較制御ステップの処理での比較結果に基づいて、第1の情報処理装置との認証処理の実行を制御する認証制御ステップとを実行させる。

【0040】本発明の第3の情報処理装置は、オンオフを入力する入力手段と、入力手段によりオンが入力された第1のタイミングを計測する第1のタイミング計測手段と、入力手段によりオフが入力された第2のタイミングを計測する第2のタイミング計測手段と、第1のタイミング、または、第2のタイミングをネットワークを介して他の情報処理装置に送信する送信手段と、他の情報処理装置より送信されてくる、送信手段により送信された第1のタイミング、または、第2のタイミングのいずれかに対応した、他の情報処理装置の他の入力手段によりオンが入力された第3のタイミング、または、オフが入力された第4のタイミングを受信する受信手段と、第1のタイミングと第3のタイミング、または、第2のタイミングと第4のタイミングとを比較する比較手段と、比較手段の比較結果に基づいて、他の情報処理装置との認証処理を実行する認証手段とを備えることを特徴とする。

【0041】前記ネットワークは、ブルートゥースにより構成されるようにすることができる。

【0042】前記第1のタイミング計測手段、および、第2のタイミング計測手段には、いずれも複数回数のタイミングを計測させ、受信手段には、他の入力手段により複数回数オンが入力された第3のタイミング、および、複数回数オフにされた第4のタイミングを受信させるようにすることができる。

【0043】前記比較手段には、第1のタイミングと第3のタイミング、または、第2のタイミングと第4のタイミングとの差を求めて、差が所定範囲内になるか否かを比較させるようにすることができる。

【0044】前記認証手段には、差が、所定の範囲内であるとき、他の情報処理装置を認証させるようにすることができる。

【0045】本発明の第3の情報処理方法は、オンオフを入力する入力ステップと、入力ステップの処理でオン

が入力された第1のタイミングを計測する第1のタイミング計測ステップと、入力ステップの処理でオフが入力された第2のタイミングを計測する第2のタイミング計測ステップと、第1のタイミング、または、第2のタイミングをネットワークを介して他の情報処理装置に送信する送信ステップと、他の情報処理装置より送信されてくる、送信ステップの処理で送信された第1のタイミング、または、第2のタイミングのいずれかに対応した、他の情報処理装置の他の入力ステップの処理でオンが入力された第3のタイミング、または、オフが入力された第4のタイミングを受信する受信ステップと、第1のタイミングと第3のタイミング、または、第2のタイミングと第4のタイミングとを比較する比較ステップと、比較ステップの処理での比較結果に基づいて、他の情報処理装置との認証処理を実行する認証ステップとを含むことを特徴とする。

【0046】本発明の第4の記録媒体のプログラムは、オンオフの入力を制御する入力制御ステップと、入力制御ステップの処理でオンが入力された第1のタイミングの計測を制御する第1のタイミング計測制御ステップと、入力制御ステップの処理でオフが入力された第2のタイミングの計測を制御する第2のタイミング計測制御ステップと、第1のタイミング、または、第2のタイミングのネットワークを介した他の情報処理装置への送信を制御する送信制御ステップと、他の情報処理装置より送信されてくる、送信制御ステップの処理で送信された第1のタイミング、または、第2のタイミングのいずれかに対応した、他の情報処理装置の他の入力制御ステップの処理でオンが入力された第3のタイミング、または、オフが入力された第4のタイミングを受信を制御する受信制御ステップと、第1のタイミングと第3のタイミング、または、第2のタイミングと第4のタイミングとの比較を制御する比較制御ステップと、比較制御ステップの処理での比較結果に基づいて、他の情報処理装置との認証処理の実行を制御する認証制御ステップとを含むことを特徴とする。

【0047】本発明の第4のプログラムは、オンオフの入力を制御する入力制御ステップと、入力制御ステップの処理でオンが入力された第1のタイミングの計測を制御する第1のタイミング計測制御ステップと、入力制御ステップの処理でオフが入力された第2のタイミングの計測を制御する第2のタイミング計測制御ステップと、第1のタイミング、または、第2のタイミングのネットワークを介した他の情報処理装置への送信を制御する送信制御ステップと、他の情報処理装置より送信されてくる、送信制御ステップの処理で送信された第1のタイミング、または、第2のタイミングのいずれかに対応した、他の情報処理装置の他の入力制御ステップの処理でオンが入力された第3のタイミング、または、オフが入力された第4のタイミングを受信を制御する受信制御ス

テップと、第1のタイミングと第3のタイミング、または、第2のタイミングと第4のタイミングとの比較を制御する比較制御ステップと、比較制御ステップの処理での比較結果に基づいて、他の情報処理装置との認証処理の実行を制御する認証制御ステップとを実行させる。

【0048】本発明の第2の情報処理システムは、第1の情報処理装置が、第2の情報処理装置より送信されてくる、第3のタイミングを受信する第1の受信手段と、第1のタイミングと第3のタイミングを比較する第1の比較手段と、第1の比較手段の比較結果に基づいて、第2の情報処理装置との認証処理を実行する第1の認証手段とを備え、第2の情報処理装置が、第1の情報処理装置より送信されてくる、第2のタイミングを受信する第2の受信手段と、第2のタイミングと第4のタイミングを比較する第2の比較手段と、第2の比較手段の比較結果に基づいて、第1の情報処理装置との認証処理を実行する第2の認証手段とを備えることを特徴とする。

【0049】本発明の第2の情報処理システムの情報処理方法は、第1の情報処理装置の情報処理方法が、第2の情報処理装置より送信されてくる、第3のタイミングを受信する第1の受信ステップと、第1のタイミングと第3のタイミングを比較する第1の比較ステップと、第1の比較ステップの処理での比較結果に基づいて、第2の情報処理装置との認証処理を実行する第1の認証ステップとを含み、第2の情報処理装置の情報処理方法が、第1の情報処理装置より送信されてくる、第2のタイミングを受信する第2の受信ステップと、第2のタイミングと第4のタイミングを比較する第2の比較ステップと、第2の比較ステップの処理での比較結果に基づいて、第1の情報処理装置との認証処理を実行する第2の認証ステップとを含むことを特徴とする。

【0050】本発明の第5の記録媒体のプログラムは、第1の情報処理装置を制御するプログラムが、第2の情報処理装置より送信されてくる、第3のタイミングを受信を制御する第1の受信制御ステップと、第1のタイミングと第3のタイミングとの比較を制御する第1の比較制御ステップと、第1の比較制御ステップの処理での比較結果に基づいて、第2の情報処理装置との認証処理の実行を制御する第1の認証制御ステップとを含み、第2の情報処理装置を制御するプログラムが、第1の情報処理装置より送信されてくる、第2のタイミングを受信を制御する第2の受信制御ステップと、第2のタイミングと第4のタイミングとの比較を制御する第2の比較制御ステップと、第2の比較制御ステップの処理での比較結果に基づいて、第1の情報処理装置との認証処理の実行を制御する第2の認証制御ステップとを含むことを特徴とする。

【0051】本発明の第5のプログラムは、第1の情報処理装置を制御するコンピュータに、第2の情報処理装置より送信されてくる、第3のタイミングを受信を制御

する第1の受信制御ステップと、第1のタイミングと第3のタイミングとの比較を制御する第1の比較制御ステップと、第1の比較制御ステップの処理での比較結果に基づいて、第2の情報処理装置との認証処理の実行を制御する第1の認証制御ステップとを実行させ、第2の情報処理装置を制御するコンピュータに、第1の情報処理装置より送信されてくる、第2のタイミングの受信を制御する第2の受信制御ステップと、第2のタイミングと第4のタイミングとの比較を制御する第2の比較制御ステップと、第2の比較制御ステップの処理での比較結果に基づいて、第1の情報処理装置との認証処理の実行を制御する第2の認証制御ステップとを実行させる。

【0052】本発明の第1の情報処理装置および方法、並びにプログラムにおいては、オンオフが入力され、オンが入力された第1のタイミングが計測され、オフが入力された第2のタイミングが計測され、第1のタイミング、および、第2のタイミングがネットワークを介して他の情報処理装置に送信される。

【0053】本発明の第2の情報処理装置および方法、並びにプログラムにおいては、オンオフが入力され、オンが入力された第1のタイミングが計測され、オフが入力された第2のタイミングが計測され、他の情報処理装置より送信されてくる、他の情報処理装置にオンが入力された第3のタイミング、および、オフが入力された第4のタイミングが受信され、第1のタイミングと第3のタイミング、および、第2のタイミングと第4のタイミングが、それぞれ比較され、比較結果に基づいて、他の情報処理装置との認証処理が実行される。

【0054】本発明の第1の情報処理システムおよび方法、並びにプログラムにおいては、第1の情報処理装置により、オンオフが入力され、オンが入力された第1のタイミングが計測され、オフが入力された第2のタイミングが計測され、第1のタイミング、および、第2のタイミングがネットワークを介して第2の情報処理装置に送信され、第2の情報処理装置により、オンオフが入力され、オンが入力されたタイミングが計測され、オフが入力されたタイミングが計測され、第1の情報処理装置より送信されてくる、第1のタイミング、および、第2のタイミングが受信され、第1のタイミングと第3のタイミング、および、第2のタイミングと第4のタイミングとがそれぞれ比較され、比較結果に基づいて、第1の情報処理装置との認証処理が実行される。

【0055】本発明の第3の情報処理装置および方法、並びにプログラムにおいては、オンオフが入力され、オンが入力された第1のタイミングが計測され、オフが入力された第2のタイミングが計測され、第1のタイミング、または、第2のタイミングがネットワークを介して他の情報処理装置に送信され、他の情報処理装置より送信されてくる、送信された第1のタイミング、または、第2のタイミングのいずれかに対応した、他の情報処理

装置のオンが入力された第3のタイミング、または、オフが入力された第4のタイミングが受信され、第1のタイミングと第3のタイミング、または、第2のタイミングと第4のタイミングとが比較され、比較結果に基づいて、他の情報処理装置との認証処理が実行される。

【0056】本発明の第2の情報処理システムおよび方法、並びにプログラムにおいては、第1の情報処理装置により、第2の情報処理装置より送信されてくる、第3のタイミングが受信され、第1のタイミングと第3のタイミングが比較され、比較結果に基づいて、第2の情報処理装置との認証処理が実行され、第2の情報処理装置により、第1の情報処理装置より送信されてくる、第2のタイミングが受信され、第2のタイミングと第4のタイミングが比較され、比較結果に基づいて、第1の情報処理装置との認証処理が実行される。

【0057】

【発明の実施の形態】図3は、本発明に係る無線通信システムの一実施の形態の構成を示す図である。尚、図3以降の図面の説明においては、従来の場合と対応する部分には同一の符号を付してあり、その説明は適宜省略する。パーソナルコンピュータ1とカムコーダ2は、上述のブルートゥースを用いることにより相互にデータを無線通信で交換することができる。

【0058】図4は、本発明を適用したパーソナルコンピュータ1とカムコーダ2の構成を示したブロック図である。まず、パーソナルコンピュータ1の構成について説明する。パーソナルコンピュータ1のマイクロコンピュータ21は、CPU（Central Processing Unit）、ROM（Read Only Memory）、および、RAM（Random Access Memory）から構成されており、CPUが、ROMに記憶されたプログラムを適宜RAMに読込んで、各種の処理を実行する。また、マイクロコンピュータ21は、パーソナルコンピュータ1の全体の動作を制御しており、バス27を介してハードディスク22に記憶されている、認証プログラム22aを始めとした各種のプログラムを内部のRAMに展開させて、各種の処理を実行する。さらに、マイクロコンピュータ21は、バス27を介してドライブ201に装着された磁気ディスク211、光ディスク212、光磁気ディスク213、または、半導体メモリ214に記憶された各種のプログラムを読込んで実行すると共に、必要に応じて、各種のプログラムやデータを書き込む。

【0059】ハードディスク22は、通信部25により接続されるカムコーダ2などの電子機器間の認証処理を実行する認証プログラム22aを始めとして、各種のプログラムを記憶すると共に、プログラムの実行に必要なデータを記憶する。表示部23は、マイクロコンピュータ21により制御され、CRT（Cathode Ray Tube）やLCD（Liquid Crystal Display）などからなり、各種の処理結果や、後述する操作のウィンドウを表示する。認証

プログラム22aは、認証ボタン26の押下されたタイミング、押下が終了したタイミングのそれぞれの時刻を計測し、これをカムコード2より送信されてくる、同様のタイミングの時刻とを、カムコード2の基準時刻と自らの基準時刻との時間差を考慮して比較し、比較結果に基づいて認証処理を実行する。PC1の自らの基準時刻は、図示せぬリアルタイムクロックより発生されている。

【0060】入力部24は、キーボードやマウスなどからなりユーザが、各種のコマンドを入力するとき操作される。通信部25は、いわゆるブルートゥースにより構成されており、マイクロコンピュータ21からの指令に基づいて、無線によりカムコード2を始めとした電子機器と各種データの授受を実行する。認証ボタン26は、認証しようとするカムコード2と、ブルートゥースにより規定された最初の認証処理を行うとき、認証しようとするカムコード2に設けられた認証ボタン35と同時に操作され、同じタイミングでオンオフされることにより、認証処理を実行させるためのものである。認証ボタン26、35の操作の詳細については後述する。

【0061】次に、カムコード2の構成について説明する。カムコード2のマイクロコンピュータ31は、カムコード2の全体の動作を制御しており、CPU、ROM、および、RAMから構成されている。マイクロコンピュータ31のCPUは、ROMに記憶された各種のプログラムを適宜RAMに読込んで各種の処理を実行する。また、マイクロコンピュータ31は、バス41に接続されたハードディスク32に記憶された、認証プログラム32aを始めとして、各種のプログラムを読込んで実行する。認証プログラム32aは、認証ボタン35の押下されたタイミング、押下が終了したタイミングのそれぞれの時刻を計測し、これらをPC1より送信されてくる、同様のタイミングを示す時刻と、PC1の基準時刻と自らの基準時刻との時間差を考慮して比較し、比較結果に基づいて認証処理を実行する。カムコード2の自らの基準時刻は、図示せぬリアルタイムクロックより発生されている。

【0062】表示部33は、撮像部34により撮像された画像や、メカデッキ39に装着された記録媒体に記録された画像を表示させる。撮像部34は、CCD (Charge Coupled Device) カメラなどからなり、図示せぬ被写体を撮像して画像データを生成する。通信部36は、上述と同様のブルートゥースから構成されており、マイクロコンピュータ31により制御され、無線通信によりPC1と各種のデータを授受する。

【0063】入力部37は、タブレットボタンなどから構成されており、ユーザが、各種のコマンドを入力するとき操作される。記録再生制御部38は、マイクロコンピュータ31からの指令に基づいて、撮像部34により撮像された画像・音声データを所定の方式で圧縮して、メカデッキ39に装着された記録媒体に記録すると共

に、記録媒体に記録された圧縮された画像・音声データを伸長し、元の画像・音声データとして再生して、表示部33に表示する。

【0064】次に、PC1の認証ボタン26と、カムコード2の認証ボタン35の認証操作について説明する。認証を行う際、ユーザは、認証させようとするPC1とカムコード2のそれぞれに設けられた認証ボタン26、35を、同じタイミングで押下する。双方の認証プログラム22a、32aは、相互の認証ボタン26、35が押下された時刻と、押下が終了された時刻をそれぞれ相互に測定し、無線通信により相互に授受し、同じタイミングで押下されたことが認識されると、認証が成立するというものである。すなわち、相互認証しようとする電子機器同士でなければ、認証ボタン26、35が同じタイミングで押下される可能性は、極めて低く、逆に、相互の認証ボタン26、35が同じタイミングで操作されれば、相互に認証処理がなされているものとみなし、認証を成立させるというものである。

【0065】ただし、ユーザによる操作であるため（人間により操作されるものである）、それぞれの認証ボタン26、35を同時に押下したつもりでも、厳密に同じタイミングで押下することはできないことがある。そこで、タイミングには、余裕を持たせてある。

【0066】すなわち、図5 (A) に示すように、PC1の認証ボタン26が押下されたタイミングをタイミングtA1とし、認証ボタン26の押下が終了したタイミングをタイミングtA2であるとし、さらに、カムコード2の認証ボタン35の押下されたタイミングをタイミングtB1とし、押下が終了したタイミングをタイミングtB2とする。この場合、例えば、カムコード2の認証ボタン35が押下されたタイミングを基準とすると、前後に時間 $e$  ( $=200\text{ms}$ 程度)の余裕を持たせて、タイミングtA1が、 $tB1 - e < tA1 < tB1 + e$ を満たし、かつ、時刻tA2が、 $tB2 - e < tA2 < tB2 + e$ を満たすとき、双方の認証ボタン26、35は、同時に押下されたものとみなす。これにより、押下されたタイミング（時刻）が、ユーザの（人間の）操作により生じてしまう程度の誤差範囲内で同時に押下されれば、相互の電子機器は認証を成立させることができる。尚、以上の説明においては、カムコード2の認証ボタン35が押下されたタイミングを基準として説明してきたが、当然のことながら、PC1の認証ボタン26が押下されたタイミングを基準としても同様である。また、上述の例では、PC1、および、カムコード2の相互に認証用の専用ボタンである認証ボタン26、35をそれぞれに操作した場合について説明してきたが、必ずしも専用のボタンを設ける必要はなく、例えば、PC1については、キーボードの所定のボタンを押下することで代用させるようにしてもよいし、カムコード2については、停止ボタンなどの認証処理時に動作に寄与しないボタンな

どで代用させるようにしても良い。認証ボタン26, 35は、押下できるもの、或いは、オンオフを切替えられるものであれば、必ずしもボタンでなくても良く、例えば、ジョグダイヤルに代表される、回転押圧式操作素子などにより認証ボタン26, 35を代用させるようにしても良いし、タッチパネルなどにより、ユーザに触れられているか否かによりオンオフが切替えられるものであればよい。

【0067】次に、図6のフローチャートを参照して、PC1とカムコード2が認証処理を実行するときの動作について説明する。

【0068】ステップS41において、PC1の認証プログラム22aは、認証ボタン26がオンにされたか（押下されたか）否かを判定し、オンにされたと判定されるまで同様の処理を繰り返し、認証ボタン26がオンにされたと判定された場合、ステップS42において、認証プログラム22aは、認証ボタン26がオンにされた、すなわち、押下されたタイミングである時刻tA1を測定し記憶する。

【0069】ステップS43において、PC1の認証プログラム22aは、認証ボタン26がオフにされたか（押下された状態が解除されたか）否かを判定し、オフにされたと判定されるまで同様の処理を繰り返し、認証ボタン26がオフにされたと判定された場合、ステップS44において、認証プログラム22aは、認証ボタン26がオフにされた、すなわち、押下された状態が解除されたタイミングである時刻tA2を測定し記憶する。

【0070】このとき、ステップS61乃至S64において、カムコード2の認証プログラム32aもPC1の認証プログラム22aと同様の処理を実行する。すなわち、ステップS61において、カムコード2の認証プログラム32aは、認証ボタン35がオンにされたか（押下されたか）否かを判定し、オンにされたと判定される

$$tB1(\text{補正後}) = tB1(\text{補正前}) - (tB0 - tA0) \cdots (1)$$

$$tB2(\text{補正後}) = tB2(\text{補正前}) - (tB0 - tA0) \cdots (2)$$

【0074】ステップS46において、認証プログラム22aは、通信部25を制御して、時刻tA1, tA2をカムコード2に送信する。

【0075】ステップS67において、カムコード2の認証プログラム32aは、PC1より時刻tA1, tA2の情報を受信したか否かを判定し、受信するまでその処理を繰り返し、受信したと判定した場合、その処理は、ステップS68に進む。

【0076】ステップS68において、認証プログラム32aは、tA1が $tB1 - e < tA1 < tB1 + e$ を満たしているか否かを判定し、例えば、図5に示すように、満たしていると判定された場合、その処理は、ステップS69に進む。

【0077】ステップS69において、認証プログラム32aは、tA2が $tB2 - e < tA2 < tB2 + e$ を

まで同様の処理を繰り返し、認証ボタン35がオンにされたと判定された場合、ステップS62において、認証プログラム32aは、認証ボタン35がオンにされた、すなわち、押下されたタイミングである時刻tB1を測定し記憶する。

【0071】ステップS63において、カムコード2の認証プログラム32aは、認証ボタン35がオフにされたか（押下された状態が解除されたか）否かを判定し、オフにされたと判定されるまで同様の処理を繰り返し、認証ボタン35がオフにされたと判定された場合、ステップS64において、認証プログラム32aは、認証ボタン35がオフにされた、すなわち、押下された状態が解除されたタイミングである時刻tB2を測定し記憶する。

【0072】ステップS45において、PC1の認証プログラム22aは、通信部25を制御して、基準時刻tA0をカムコード2に送信する。

【0073】ステップS65において、カムコード2の認証プログラム32aは、通信部36を制御して、基準タイミングtA0を受信したか否かを判定し、基準時刻tA0が受信されるまで、その処理を繰り返し、受信したと判定された場合、ステップS66において、自らの基準時刻との時間差（ $tB0 - tA0$ ）を演算し、時刻tB1, tB2を補正する。すなわち、PC1で計測されたタイミングとカムコード2で計測されたタイミングを比較することになるので、PC1の基準時刻、すなわち、例えば、基準時刻を送信する際のPC1のリアルタイムクロックで計測された時刻tA0を送信すると、カムコード2は、これを受信し、自らの基準時刻tB0との差を求めて、PC1との時間差を求め、これを利用して、以下の式（1）、式（2）に示すように、自らが計測した時刻tB1, tB2から、その時間差を減算して求める。

満たしているか否かを判定し、例えば、図5に示すように、満たしていると判定された場合、ステップS70において、認証が認められたことをPC1に通知する。

【0078】ステップS47において、PC1の認証プログラム22aは、通知を受信したか否かを判定し、通知が受信されるまで同様の処理を繰り返し、例えば、ステップS70の処理により、認証が認められた通知が受信されると、ステップS48において、PC1の認証プログラム22aは、認証結果を認識し、今の場合、認証が認められたことを認識する。

【0079】ステップS68, S69において、tA1が $tB1 - e < tA1 < tB1 + e$ を満たしていない、または、tA2が $tB2 - e < tA2 < tB2 + e$ を満たしていないと判定された場合、ステップS71において、認証プログラム32aは、認証が認められなかつ

た、すなわち、認証ボタン26, 35が同時に操作されなかったとみなし、通信部36を制御して、認証が認められなかったことをPC1に通知する。

【0080】以上の例においては、カムコード2側でPC1とカムコード2の認証ボタン26, 35が同時に操作されたかを認証判定する処理について説明してきたが、当然のことながら、PC1側で認証判定処理(図6のステップS68, 69の処理)を実行するようにしてもよい。

【0081】また、認証判定処理は、PC1とカムコード2で、相互に実行するようにしてもよく、その場合の処理について、図7のフローチャートを参照して説明する。

【0082】ステップS81において、PC1の認証プログラム22aは、認証ボタン26がオンにされたか(押下されたか)否かを判定し、オンにされたと判定されるまで同様の処理を繰り返し、認証ボタン26がオンにされたと判定された場合、ステップS82において、認証プログラム22aは、認証ボタン26がオンにされた、すなわち、押下されたタイミングである時刻tA1を測定し記憶する。

【0083】ステップS83において、PC1の認証プログラム22aは、認証ボタン26がオフにされたか(押下された状態が解除されたか)否かを判定し、オフにされたと判定されるまで同様の処理を繰り返し、認証ボタン26がオフにされたと判定された場合、ステップS84において、認証プログラム22aは、認証ボタン26がオフにされた、すなわち、押下された状態が解除されたタイミングである時刻tA2を測定し記憶する。

【0084】このとき、ステップS101乃至S104において、カムコード2の認証プログラム32aもPC1の認証プログラム22aと同様の処理を実行する。すなわち、ステップS101において、カムコード2の認証プログラム32aは、認証ボタン35がオンにされたか(押下されたか)否かを判定し、オンにされたと判定されるまで同様の処理を繰り返し、認証ボタン35がオンにされたと判定された場合、ステップS102において、認証プログラム32aは、認証ボタン35がオンにされた、すなわち、押下されたタイミングである時刻tB1を測定し記憶する。

【0085】ステップS103において、カムコード2の認証プログラム32aは、認証ボタン35がオフにされたか(押下された状態が解除されたか)否かを判定し、オフにされたと判定されるまで同様の処理を繰り返し、認証ボタン35がオフにされたと判定された場合、ステップS104において、認証プログラム32aは、認証ボタン35がオフにされた、すなわち、押下された状態が解除されたタイミングである時刻tB2を測定し記憶する。

【0086】ステップS85において、PC1の認証プロ

グラム22aは、通信部25を制御して、基準時刻tA0をカムコード2に送信する。

【0087】ステップS105において、カムコード2の認証プログラム32aは、通信部36を制御して、基準タイミングtA0を受信したか否かを判定し、基準時刻tA0を受信されるまで、その処理を繰り返し、受信したと判定された場合、ステップS106において、自らの基準時刻との時間差( $tB0 - tA0$ )を演算し、時刻tB1, tB2を補正する。

【0088】ステップS86において、認証プログラム22aは、通信部25を制御して、時刻tA1, tA2をカムコード2に送信する。

【0089】ステップS107において、カムコード2の認証プログラム32aは、PC1より時刻tA1, tA2の情報を受信したか否かを判定し、受信するまでその処理を繰り返し、受信したと判定した場合、その処理は、ステップS108に進む。

【0090】ステップS108において、認証プログラム32aは、 $tA1$ が $tB1 - e < tA1 < tB1 + e$ を満たしているか否かを判定し、例えば、図8(B)に示すように、満たしていると判定された場合、その処理は、ステップS109に進む。

【0091】ステップS109において、認証プログラム32aは、通信部36を制御して、認証が認められたことをPC1に通知する。

【0092】ステップS87において、PC1の認証プログラム22aは、通知を受信したか否かを判定し、通知を受信されるまで同様の処理を繰り返し、例えば、ステップS109の処理により、認証が認められた通知を受信されると、その処理は、ステップS88に進む。

【0093】ステップS110において、認証プログラム32aは、通信部36を制御して、時刻tB2をPC1に送信する。

【0094】ステップS88において、PC1の認証プログラム22aは、通信部25を制御して、時刻tB2をカムコード2より受信したか否かを判定し、受信されるまで、その処理を繰り返し、受信されたと判定された場合、その処理は、ステップS89に進む。

【0095】ステップS89において、認証プログラム22aは、 $tB2$ が $tA2 - e < tB2 < tA2 + e$ を満たしているか否かを判定し、例えば、図8(A)に示すように、満たしていると判定された場合、ステップS90において、通信部25を制御して、認証が認められたことをカムコード2に通知する。

【0096】ステップS111において、カムコード2の認証プログラム32aは、PC1から送信されてくる認証結果を受信し、認識する。例えば、ステップS90の処理により送信されてくる認証結果により認証が認められたことを認識する。

【0097】ステップS108において、tA1がtB



$1 - e < tA1 < tB1 + e$ を満たしていないと判定された場合、ステップS112において、認証プログラム32aは、認証が認められなかった、すなわち、認証ボタン26、35が同時に操作されなかったとみなし、通信部36を制御して、認証が認められなかったことをPC1に通知する。

【0098】結果として、ステップS87において、認証プログラム22aは、認証が認められなかったと判定し、その処理は終了する。

【0099】また、ステップS89において、 $tB2$ が  $tA2 - e < tB2 < tA2 + e$ を満たしていないと判定された場合、ステップS91において、PC1の認証プログラム22aは、通信部25を制御して認証が認められなかったことをカムコード2に送信する。

【0100】以上のように、カムコード2では、認証ボタン26、35が押下されたタイミングの時刻が比較され、PC1では、認証ボタン26、35の押下が解除されたタイミングの時刻が比較されることにより、相互で認証処理を行うことができる。もちろん、以上の例とは、逆に、PC1が、認証ボタン26、35が押下されたタイミングの時刻を比較し、カムコード2が、認証ボタン26、35の押下が解除されたタイミングの時刻を比較するようにしてもよい。

【0101】また、以上の例においては、認証ボタン26、35が相互に1回だけ押下された場合の処理について説明してきたが、1回の押下では、誤操作などにより偶然に認証が認められてしまう可能性がある。このため、認証ボタン26、35を押下する回数は、複数回数にするようにして、誤操作の発生を防止させることもできる。

【0102】そこで、次に、認証ボタン26、35を相互に複数回数ずつ押下する場合（例えば、 $n$ 回押下する場合）について、図9のフローチャートを参照して説明する。このとき、認証プログラム22a、32aは、押下された回数をカウントするためのカウンタ $i$ をそれぞれ備える。

【0103】ステップS121において、PC1の認証プログラム22aは、自らのカウンタ $i$ を1に初期化する。ステップS122において、PC1の認証プログラム22aは、認証ボタン26がオンにされたか（押下されたか）否かを判定し、オンにされたと判定されるまで同様の処理を繰り返し、認証ボタン26がオンにされたと判定された場合、ステップS123において、認証プログラム22aは、認証ボタン26がオンにされた、すなわち、押下されたタイミングである時刻 $tAi$ を測定し記憶する。

【0104】ステップS124において、PC1の認証プログラム22aは、認証ボタン26がオフにされたか（押下された状態が解除されたか）否かを判定し、オフにされたと判定されるまで同様の処理を繰り返し、認証

ボタン26がオフにされたと判定された場合、ステップS125において、認証プログラム22aは、認証ボタン26がオフにされた、すなわち、押下された状態が解除されたタイミングである時刻 $tA(i+1)$ を測定し記憶する。ステップS126において、認証プログラム22aは、カウンタ $i$ を2だけインクリメントする。ステップS127において、カウンタ $i/2$ が $n$ より大きいと判定された場合、カウンタ $i/2$ が $n$ より大きくないと判定された場合、その処理は、ステップS122に戻りそれ以降の処理が繰り返され、認証ボタン26が押下されるべき設定回数である $n$ よりも $i/2$ が大きくなるまで、ステップS122乃至S126の処理が繰り返される。ステップS127において、カウンタ $i/2$ が認証ボタン26が押下される所定回数 $n$ より大きいと判定された場合、その処理は、ステップS128に進む。

【0105】このとき、ステップS141乃至S147において、カムコード2の認証プログラム32aもPC1の認証プログラム22aと同様の処理を実行する。すなわち、ステップS141において、カムコード2の認証プログラム32aは、自らのカウンタ $i$ を1に初期化する。ステップS142において、カムコード2の認証プログラム32aは、認証ボタン35がオンにされたか（押下されたか）否かを判定し、オンにされたと判定されるまで同様の処理を繰り返し、認証ボタン35がオンにされたと判定された場合、ステップS143において、認証プログラム32aは、認証ボタン35がオンにされた、すなわち、押下されたタイミングである時刻 $tBi$ を測定し記憶する。

【0106】ステップS144において、カムコード2の認証プログラム32aは、認証ボタン35がオフにされたか（押下された状態が解除されたか）否かを判定し、オフにされたと判定されるまで同様の処理を繰り返し、認証ボタン35がオフにされたと判定された場合、ステップS145において、認証プログラム32aは、認証ボタン35がオフにされた、すなわち、押下された状態が解除されたタイミングである時刻 $tB(i+1)$ を測定し記憶する。

【0107】ステップS146において、カムコード2の認証プログラム32aは、カウンタ $i$ を2だけインクリメントする。ステップS147において、カウンタ $i/2$ が $n$ より大きいと判定された場合、カウンタ $i/2$ が $n$ より大きくないと判定された場合、その処理は、ステップS142に戻りそれ以降の処理が繰り返され、認証ボタン26が押下されるべき設定回数である $n$ よりも $i/2$ が大きくなるまで、ステップS142乃至S146の処理が繰り返される。ステップS147において、カウンタ $i/2$ が認証ボタン35が押下される所定回数 $n$ より大きいと判定された場合、その処理は、ステップS148に進む。

【0108】ステップS128において、PC1の認証プ



ログラム22aは、通信部25を制御して、基準時刻 $t_{A0}$ をカムコード2に送信する。

【0109】ステップS148において、カムコード2の認証プログラム32aは、通信部36を制御して、基準タイミング $t_{A0}$ を受信したか否かを判定し、基準時刻 $t_{A0}$ が受信されるまで、その処理を繰り返し、受信したと判定された場合、ステップS149において、自らの基準時刻との時間差( $t_{B0}-t_{A0}$ )を演算し、時刻 $t_{B1}$ ,  $t_{B2}$ ...,  $t_{B(2n)}$ を補正する。

【0110】ステップS129において、認証プログラム22aは、通信部25を制御して、時刻 $t_{A1}$ ,  $t_{A2}$ ...,  $t_{A(2n)}$ をカムコード2に送信する。

【0111】ステップS150において、カムコード2の認証プログラム32aは、PC1より時刻 $t_{A1}$ ,  $t_{A2}$ ...,  $t_{A(2n)}$ の情報を受信したか否かを判定し、受信するまでその処理を繰り返し、受信したと判定した場合、その処理は、ステップS151に進む。

【0112】ステップS151において、認証プログラム32aは、全ての $i$  ( $i=1$ 乃至 $2n$ ) について、 $t_{Ai}$ が $t_{Bi}-e < t_{Ai} < t_{Bi}+e$ を満たしているか否かを判定し、例えば、図10に示すように、 $t_{B1}-e < t_{A1} < t_{B1}+e$ ,  $t_{B2}-e < t_{A2} < t_{B2}+e$ ,  $t_{B3}-e < t_{A3} < t_{B3}+e$ ,  $t_{B4}-e < t_{A4} < t_{B4}+e$ , ...  $t_{B(2n-1)}-e < t_{A(2n-1)} < t_{B(2n-1)}+e$ ,  $t_{B(2n)}-e < t_{A(2n)} < t_{B(2n)}+e$ 満たしていると判定された場合、その処理は、ステップS152に進む。ステップS152において、認証プログラム32aは、認証が認められたことをPC1に通知する。

【0113】ステップS130において、PC1の認証プログラム22aは、通知を受信したか否かを判定し、通知が受信されるまで同様の処理を繰り返し、例えば、ステップS152の処理により、認証が認められた通知が受信されると、ステップS131において、PC1の認証プログラム22aは、認証結果を認識し、今の場合、認証が認められたことを認識する。

【0114】ステップS151において、全ての $i$  ( $i=1$ 乃至 $2n$ ) について、 $t_{Ai}$ が $t_{Bi}-e < t_{Ai} < t_{Bi}+e$ を満たしていないと判定された場合、ステップS153において、認証プログラム32aは、認証が認められなかった、すなわち、認証ボタン26, 35が同時に操作されなかったとみなし、通信部36を制御して、認証が認められなかったことをPC1に通知する。

【0115】以上の例においては、カムコード2側でPC1とカムコード2の認証ボタン26, 35が、複数回数に渡って同時に操作されたかを認証判定する処理について説明してきたが、当然のことながら、PC1側で認証判定処理(図9のステップS151の処理)を実行するようにしてもよい。

【0116】また、認証ボタン26, 35を複数回数押

下する場合でも、図7のフローチャートを参照して説明したように、認証判定処理は、PC1とカムコード2で、相互に実行するようにしてもよく、その場合の処理について、図11のフローチャートを参照して説明する。

【0117】ステップS171において、PC1の認証プログラム22aは、自らのカウンタ $i$ を1に初期化する。ステップS172において、PC1の認証プログラム22aは、認証ボタン26がオンにされたか(押下されたか)否かを判定し、オンにされたと判定されるまで同様の処理を繰り返し、認証ボタン26がオンにされたと判定された場合、ステップS173において、認証プログラム22aは、認証ボタン26がオンにされた、すなわち、押下されたタイミングである時刻 $t_{Ai}$ を測定し記憶する。

【0118】ステップS174において、PC1の認証プログラム22aは、認証ボタン26がオフにされたか(押下された状態が解除されたか)否かを判定し、オフにされたと判定されるまで同様の処理を繰り返し、認証ボタン26がオフにされたと判定された場合、ステップS175において、認証プログラム22aは、認証ボタン26がオフにされた、すなわち、押下された状態が解除されたタイミングである時刻 $t_{A(i+1)}$ を測定し記憶する。

【0119】ステップS176において、認証プログラム22aは、カウンタ $i$ を2だけインクリメントする。ステップS177において、カウンタ $i/2$ が $n$ より大きいと判定された場合、その処理は、ステップS172に戻りそれ以降の処理が繰り返され、認証ボタン26が押下されるべき設定回数である $n$ よりも $i/2$ が大きくなるまで、ステップS172乃至S176の処理が繰り返される。ステップS177において、カウンタ $i/2$ が認証ボタン26が押下される所定回数 $n$ より大きいと判定された場合、その処理は、ステップS178に進む。

【0120】このとき、ステップS201乃至S207において、カムコード2の認証プログラム32aもPC1の認証プログラム22aと同様の処理を実行する。すなわち、ステップS201において、カムコード32aは、カウンタ $i$ を1に初期化する。さらに、ステップS202において、カムコード2の認証プログラム32aは、認証ボタン35がオンにされたか(押下されたか)否かを判定し、オンにされたと判定されるまで同様の処理を繰り返し、認証ボタン35がオンにされたと判定された場合、ステップS203において、認証プログラム32aは、認証ボタン35がオンにされた、すなわち、押下されたタイミングである時刻 $t_{Bi}$ を測定し記憶する。

【0121】ステップS204において、カムコード2の認証プログラム32aは、認証ボタン35がオフにされたか(押下された状態が解除されたか)否かを判定

し、オフにされたと判定されるまで同様の処理を繰り返し、認証ボタン35がオフにされたと判定された場合、ステップS205において、認証プログラム32aは、認証ボタン35がオフにされた、すなわち、押下された状態が解除されたタイミングである時刻 $tB(i+1)$ を測定し記憶する。

【0122】ステップS206において、認証プログラム32aは、カウンタ $i$ を2だけインクリメントする。ステップS207において、カウンタ $i/2$ が $n$ より大きいかなかを判定し、カウンタ $i/2$ が $n$ より大きくないと判定された場合、その処理は、ステップS202に戻りそれ以降の処理が繰り返され、認証ボタン35が押下されるべき設定回数である $n$ よりも $i/2$ が大きくなるまで、ステップS202乃至S206の処理が繰り返される。ステップS207において、カウンタ $i/2$ が認証ボタン35が押下される所定回数 $n$ より大きいと判定された場合、その処理は、ステップS208に進む。

【0123】ステップS178において、PC1の認証プログラム22aは、通信部25を制御して、基準時刻 $tA0$ をカムコード2に送信する。

【0124】ステップS208において、カムコード2の認証プログラム32aは、通信部36を制御して、基準タイミング $tA0$ を受信したか否かを判定し、基準時刻 $tA0$ が受信されるまで、その処理を繰り返し、受信したと判定された場合、ステップS209において、自らの基準時刻との時間差( $tB0-tA0$ )を演算し、時刻 $tB1, tB2, \dots, tB(2n)$ を補正する。

【0125】ステップS179において、認証プログラム22aは、通信部25を制御して、 $tAi$ のうちカウンタ $i$ が奇数となる時刻 $tA1, tA3, \dots, tA(2n-1)$ をカムコード2に送信する。

【0126】ステップS210において、カムコード2の認証プログラム32aは、PC1より $tAi$ のうちカウンタ $i$ が奇数となる時刻 $tA1, tA3, \dots, tA(2n-1)$ の情報を受信したか否かを判定し、受信するまでその処理を繰り返し、受信したと判定した場合、その処理は、ステップS211に進む。

【0127】ステップS211において、認証プログラム32aは、全ての奇数のカウンタ $i$ ( $i=1, 3, 5, \dots, 2n-1$ )の $tAi$ について、 $tBi-e < tAi < tBi+e$ を満たしているか否かを判定し、例えば、図12(B)に示すように、 $tB1-e < tA1 < tB1+e, tB3-e < tA3 < tB3+e, \dots, tB(2n-1)-e < tA(2n-1) < tB(2n-1)+e$ を満たしていると判定された場合、その処理は、ステップS212において、認証が認められたことをPC1に通知する。

【0128】ステップS180において、PC1の認証プログラム22aは、通知を受信したか否かを判定し、通知が受信されるまで同様の処理を繰り返し、例えば、ス

テップS212の処理により、認証が認められた通知が受信されると、ステップS181に進む。

【0129】ステップS213において、認証プログラム32aは、通信部36を制御して、時刻 $tBi$ のうち、 $i$ が偶数の時刻 $tB2, tB4, \dots, tB(2n)$ をPC1に送信する。

【0130】ステップS181において、PC1の認証プログラム22aは、通信部25を制御して、時刻 $tB2, tB4, \dots, tB(2n)$ をカムコード2より受信したか否かを判定し、受信されるまで、その処理を繰り返し、受信されたと判定された場合、その処理は、ステップS182に進む。

【0131】ステップS182において、認証プログラム22aは、時刻 $tB2, tB4, \dots, tB(2n)$ が $tA2-e < tB2 < tA2+e, tA4-e < tB4 < tA4+e, \dots, tA(2n)-e < tB(2n) < tA(2n)+e$ を満たしているか否かを判定し、例えば、図12(A)に示すように、満たしていると判定された場合、ステップS183において、通信部25を制御して、認証が認められたことをカムコード2に通知する。

【0132】ステップS214において、カムコード2の認証プログラム32aは、PC1から送信されてくる認証結果を受信し、認識する。例えば、ステップS183の処理により送信されてくる認証結果により認証が認められたことを認識する。

【0133】ステップS211において、 $tAi$ のうち $i$ が奇数のものが $tBi-e < tAi < tBi+e$ を満たしていないと判定された場合、ステップS215において、認証プログラム32aは、認証が認められなかった、すなわち、認証ボタン26, 35が複数回数に渡って同時に操作されなかったとみなし、通信部36を制御して、認証が認められなかったことをPC1に通知する。

【0134】結果として、ステップS180において、認証プログラム22aは、認証が認められなかったと判定し、その処理は終了する。

【0135】また、ステップS182において、 $tBi$ のうち $i$ が偶数のものが $tAi-e < tBi < tAi+e$ を満たしていないと判定された場合、ステップS184において、PC1の認証プログラム22aは、通信部25を制御して認証が認められなかったことをカムコード2に送信する。

【0136】以上のように、複数回数に渡り、PC1とカムコード2の相互で認証処理を実行させることもでき、認証処理時の誤動作などにも対応することができる。

【0137】以上の例においては、PC1とカムコード2の間での認証処理について説明してきたが、それ以外の電子機器間でも、ブルートゥースを備えた電子機器間であればよく、例えば、図1(B)乃至(D)に示すように、ブルートゥースを備えた携帯電話機3とハンディカ

ムコード4、カムコード2と携帯情報端末機5、携帯型パーソナルコンピュータ6と携帯情報端末機5などに代表される様々な電子機器間でも、同様の処理による認証処理を実現させることができる。

【0138】また、ブルートゥースの規格においては、PIN=0とすることによりPINの入力を省略させた状態で接続することができるようになっている。このPINの省略機能を利用して、最初の認証処理は、ブルートゥースの規格通りの認証処理として、それ以降の認証処理は、上述のように認証ボタンを用いる方法とするようにしてもよい。

【0139】さらに、認証処理を実行する毎に、認証ボタン26、35の押下回数 $n$ を変化させるようにしてもよい。

【0140】また、上述の例では、PC1とカムコード2の認証プログラム22a、32aで、相互に認証処理を実行する場合、一方の認証プログラムが認証ボタン26、35が押下された時刻を比較し、他方の認証プログラムが認証ボタン26、35の押下状態が解除された時刻を比較することにより認証処理を行う例について説明してきたが、相互の認証プログラムが比較する時刻は、互いに重なり合わない時刻同士であれば、2つの集合に分けて、相互に比較するようにしてもよい。

【0141】さらに、相互の基準時刻 $tA0$ 、 $tB0$ を使用せずに、例えば、それぞれの最初に認証ボタン26、35が押下されるタイミングである時刻 $tA1$ 、 $tB1$ を基準として、各時刻との差を求めて、 $tAi - tA1$ と $tBi - tB1$ を、 $i = 1$ 乃至 $2n$ の範囲で求めて、それぞれ対応する時刻を比較するようにしてもよい。このとき、時刻 $tA1$ 、 $tB1$ は、基準時刻と同様に扱われるため、タイミングを比較する時刻の数が1個分減ることになるので、1回の押下( $n = 1$ )だけでは、認証ボタン26、35のタイミングの差を求めることができないので、複数回数の押下の開始と終了のタイミングの時刻情報が必要となる。

【0142】また、本発明は、通信部25、36としてブルートゥースを用いた例について説明してきたが、ブルートゥース以外の通信部からなる無線通信システム、または、有線通信システム上での認証処理に使用するようにしてもよい。

【0143】以上によれば、簡単な操作で、認証処理を実現させることができる。

【0144】上述した一連の処理は、ハードウェアにより実行させることもできるが、ソフトウェアにより実行させる場合にもできる。一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行させることが可能な、例えば汎用のパーソナルコンピュータなどに記録媒体からイ

ンストールされる。

【0145】この記録媒体は、図4に示すようにパーソナルコンピュータ1に予め組み込まれた状態でユーザに提供される、プログラムが記録されているハードディスク22だけではなく、コンピュータとは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク211（フレキシブルディスクを含む）、光ディスク212（CD-ROM(Compact Disc-Read Only Memory)、DVD(Digital Versatile Disc)を含む）、光磁気ディスク213（MD(Mini-Disc)（登録商標）を含む）、もしくは半導体メモリ214（Memory Stickを含む）などよりなるパッケージメディアにより構成される。

【0146】尚、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に沿って時系列的に行われる処理は、もちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理を含むものである。

【0147】また、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

【0148】

【発明の効果】本発明の第1の情報処理装置および方法、並びにプログラムによれば、オンオフを入力し、オンを入力した第1のタイミングを計測し、オフを入力した第2のタイミングを計測し、第1のタイミング、および、第2のタイミングをネットワークを介して他の情報処理装置に送信するようにした。

【0149】本発明の第2の情報処理装置および方法、並びにプログラムによれば、オンオフを入力し、オンを入力した第1のタイミングを計測し、オフを入力した第2のタイミングを計測し、他の情報処理装置より送信されてくる、他の情報処理装置にオンを入力した第3のタイミング、および、オフを入力した第4のタイミングを受信し、第1のタイミングと第3のタイミング、および、第2のタイミングと第4のタイミングを、それぞれ比較し、比較結果に基づいて、他の情報処理装置との認証処理を実行するようにした。

【0150】本発明の第1の情報処理システムおよび方法、並びにプログラムによれば、第1の情報処理装置が、オンオフを入力し、オンを入力した第1のタイミングを計測し、オフを入力した第2のタイミングを計測し、第1のタイミング、および、第2のタイミングをネットワークを介して第2の情報処理装置に送信し、第2の情報処理装置が、オンオフを入力し、オンを入力したタイミングを計測し、オフを入力したタイミングを計測し、第1の情報処理装置より送信されてくる、第1のタイミング、および、第2のタイミングを受信し、第1のタイミングと第3のタイミング、および、第2のタイミングと第4のタイミングとをそれぞれ比較し、比較結果

に基づいて、第1の情報処理装置との認証処理を実行するようにした。

【0151】本発明の第3の情報処理装置および方法、並びにプログラムによれば、オンオフを入力し、オンを入力した第1のタイミングを計測し、オフを入力した第2のタイミングを計測し、第1のタイミング、または、第2のタイミングをネットワークを介して他の情報処理装置に送信し、他の情報処理装置より送信されてくる、送信された第1のタイミング、または、第2のタイミングのいずれかに対応した、他の情報処理装置にオンを入力した第3のタイミング、または、オフを入力した第4のタイミングを受信し、第1のタイミングと第3のタイミング、または、第2のタイミングと第4のタイミングとを比較し、比較結果に基づいて、他の情報処理装置との認証処理を実行するようにした。

【0152】本発明の第2の情報処理システムおよび方法、並びにプログラムによれば、第1の情報処理装置が、第2の情報処理装置より送信されてくる、第3のタイミングを受信し、第1のタイミングと第3のタイミングを比較し、比較結果に基づいて、第2の情報処理装置との認証処理を実行し、第2の情報処理装置が、第1の情報処理装置より送信されてくる、第2のタイミングを受信し、第2のタイミングと第4のタイミングを比較し、比較結果に基づいて、第1の情報処理装置との認証処理を実行するようにした。

【0153】いずれにおいても、結果として、相互認証処理を簡単に実行することが可能となる。

【図面の簡単な説明】

【図1】従来の無線接続による電子機器の組合せを示す図である。

【図2】従来の認証処理を説明するフローチャートである。

【図3】本発明を適用した無線通信システムの一実施の形態の構成を示す図である。

【図4】図3のパーソナルコンピュータとカムコーダの構成を示すブロック図である。

【図5】認証ボタンの押下のタイミングを示すタイミングチャートである。

【図6】本発明を適用した認証処理を説明するフローチャートである。

【図7】本発明を適用した認証処理を説明するフローチャートである。

【図8】認証ボタンの押下のタイミングを示すタイミングチャートである。

【図9】本発明を適用した認証処理を説明するフローチャートである。

【図10】認証ボタンの押下のタイミングを示すタイミングチャートである。

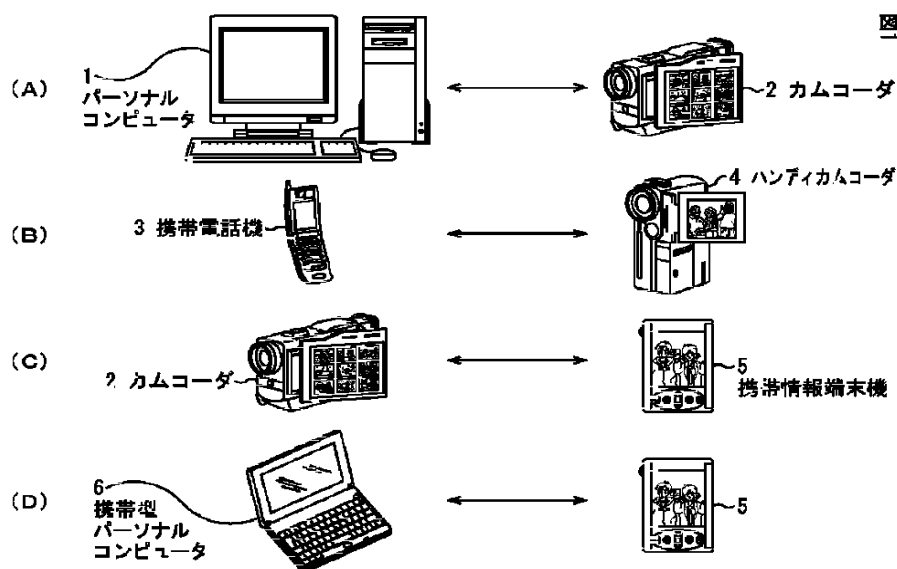
【図11】本発明を適用した認証処理を説明するフローチャートである。

【図12】認証ボタンの押下のタイミングを示すタイミングチャートである。

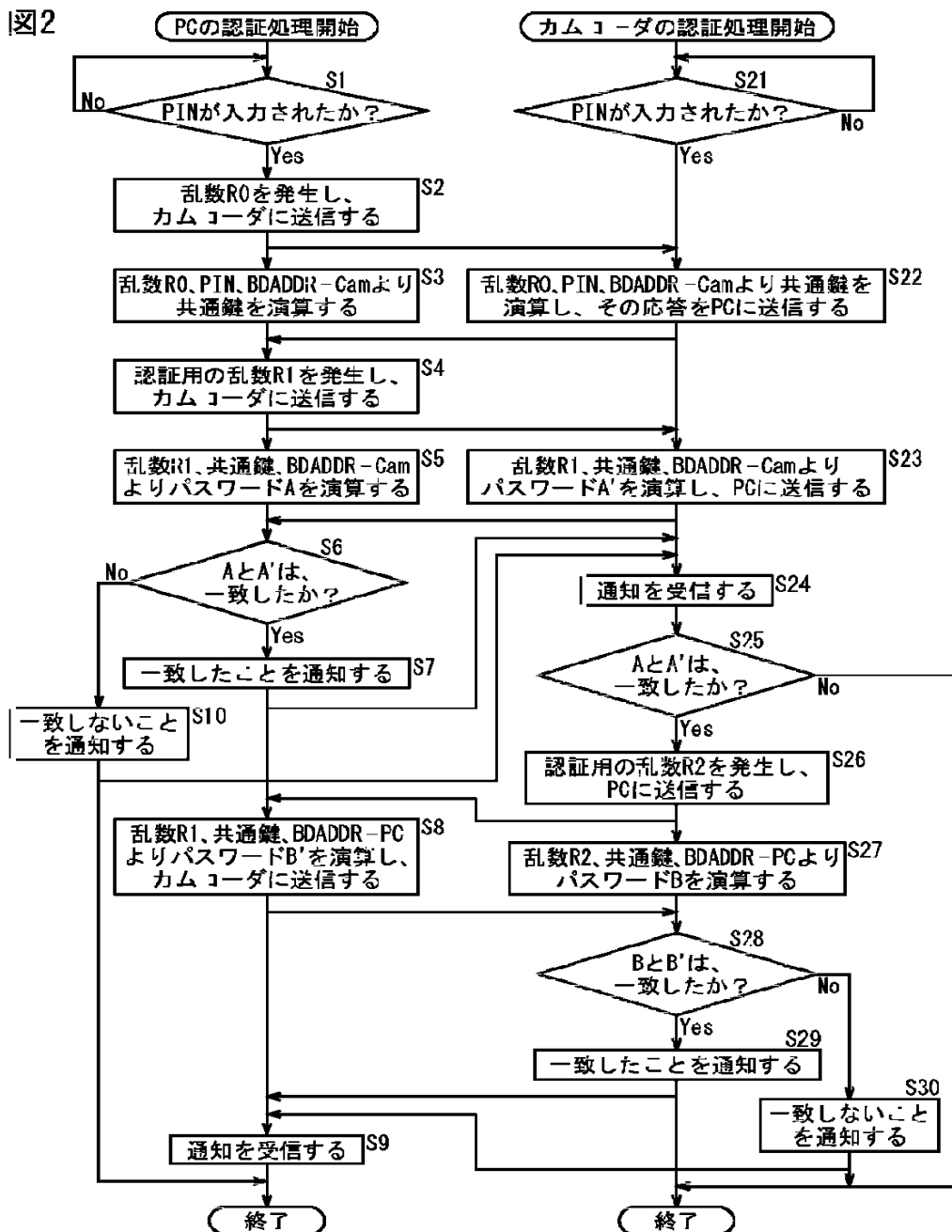
【符号の説明】

1 パーソナルコンピュータ、2 カムコーダ、22a 認証プログラム、26 認証ボタン、32a 認証プログラム、35 認証ボタン

【図1】

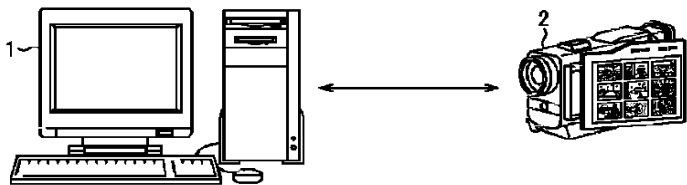


【図2】



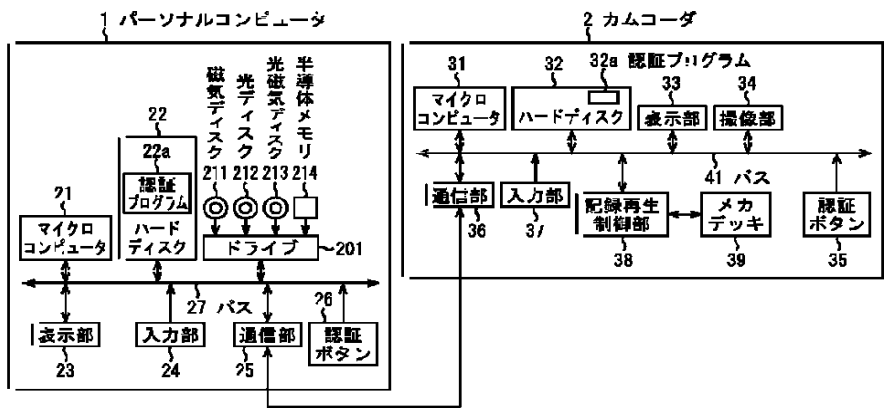
【 図 3 】

図 3



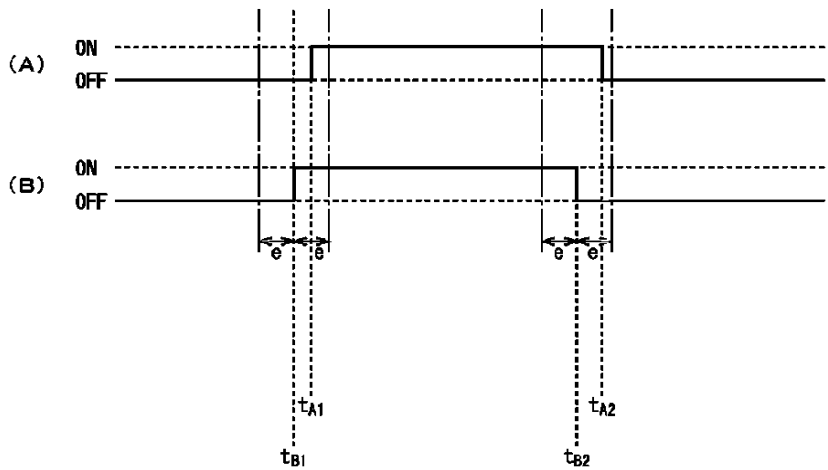
【 図 4 】

図 4

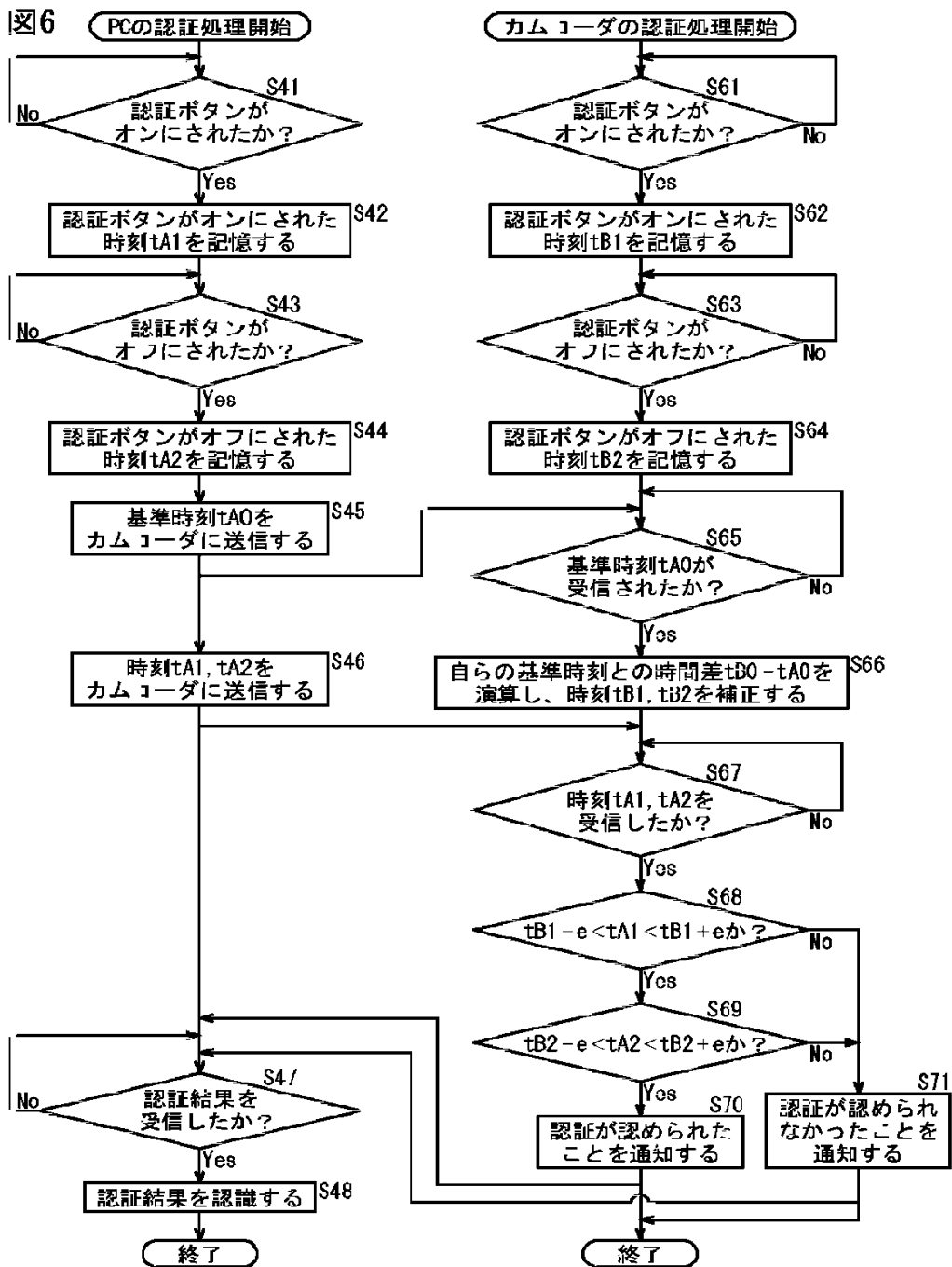


【 図 5 】

図 5

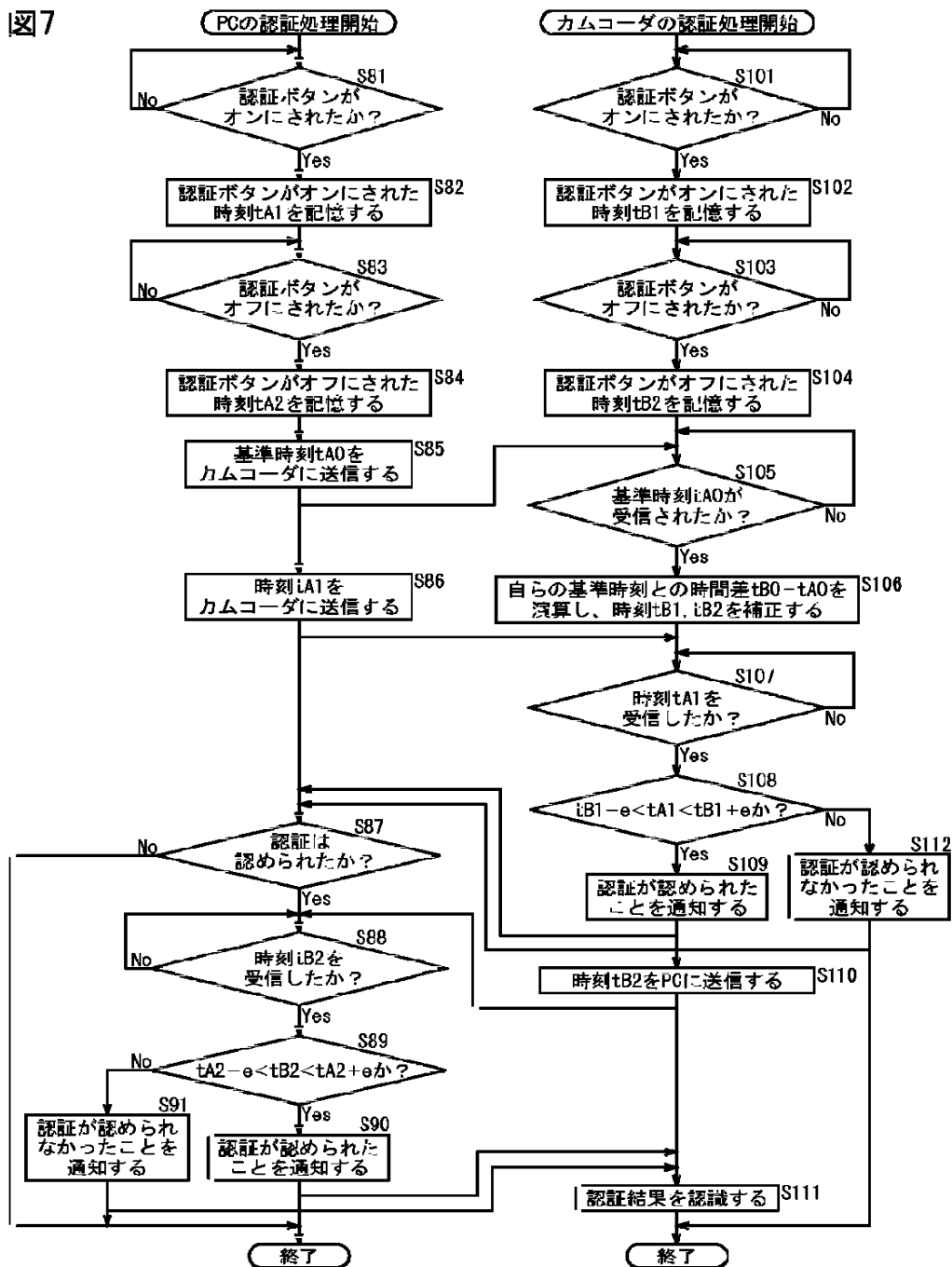


【図6】



【図7】

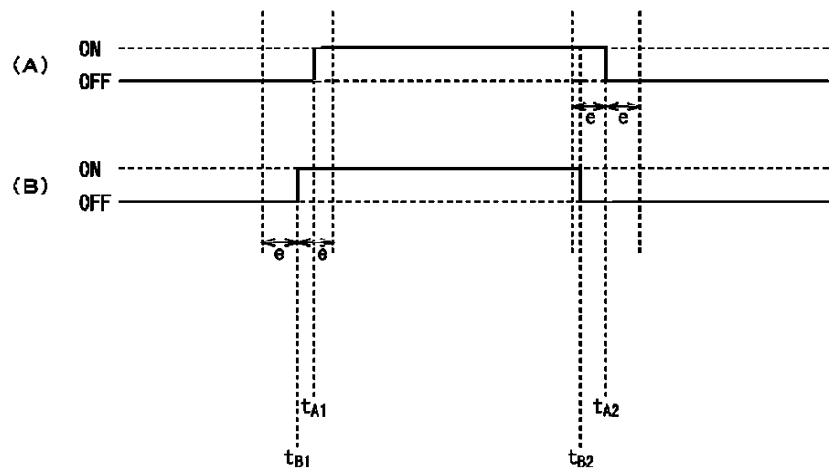
図7





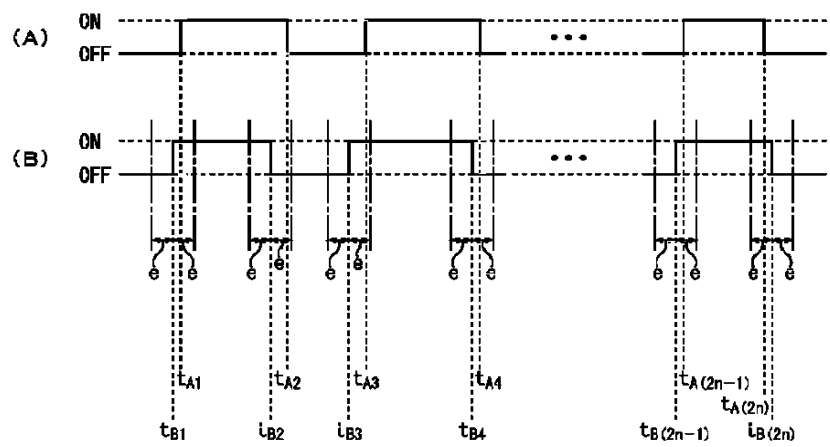
【図8】

8



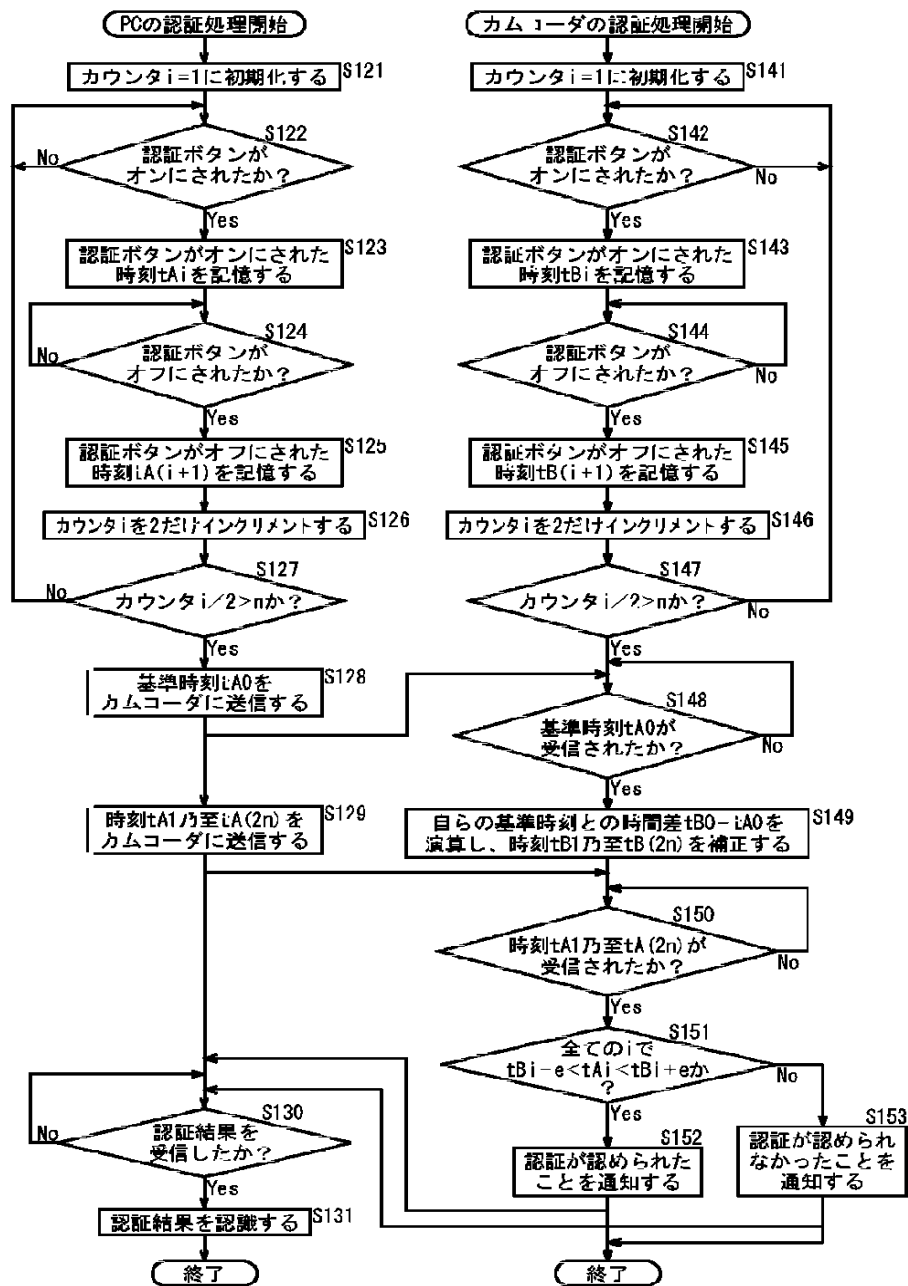
【図10】

10



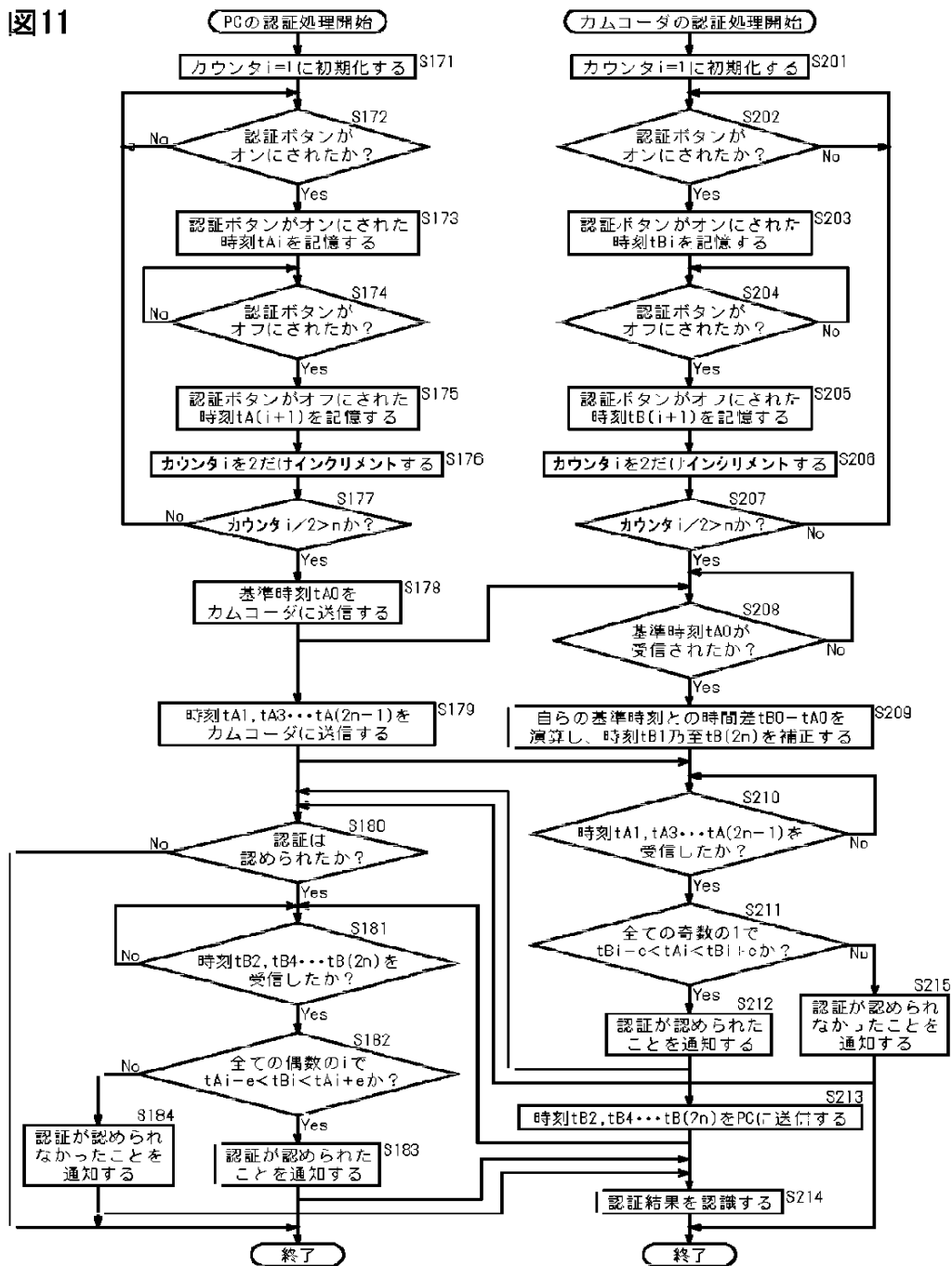
【図9】

図9



【図11】

図11



【図12】

図12

